Abstract

• Companies developing safety-related E/E products may have SPICE-compliant processes. However, this is not enough to fulfill the requirements specified by functional safety standards like the new ISO 26262. These processes definitely need an update, and the way the organization works needs a change. But how is this change best implemented in practice, at lowest possible cost, and with the highest possible success rate?

• This tutorial presents the essential steps to be taken to achieve processes and projects capable of functional safety, covering questions like:
  • How can we systematically identify what to change in which element of which process?
  • Where is there little to do, and where is a lot of work ahead?
  • What are the success factors to be considered?
  • How is the change to be organized?
  • What needs to be planned?
  • How long will it take, and what are the costs to be expected?
Contents

• Maturity models and functional safety standards
• Relationship between ISO/DIS 26262 and Automotive SPICE
• How to implement ISO/DIS 26262 requirements/clauses?
• How to implement ISO/DIS 26262 work products?
• How to achieve compliance with ISO/DIS 26262
• Timeline for functional safety compliance
• Selected elements of the program to achieve compliance
• Confirmation measures
• Success factors for achieving functional safety capability
• Cost considerations

Initial Situation
What are the challenges?

• Customers expect safe products
• Highly complex safety-related electronic products endanger life
• Safe products are legally required
• Need to avoid liability claims and be compliant to safety standards
  • For Automotive E/E products ISO 26262 will be considered state-of-the-art technique in 2011
• Not all organizations are already set up to fully comply with safety standards and able to achieve safety goals
  • Processes
  • Product architecture (hardware, software)
  • Skilled staff
Maturity Models and Functional Safety Standards

Functional Safety and Maturity Models
They support each other

- Requirements from IEC 61508 / ISO/DIS 26262
- Requirements from CMMI / SPICE

<table>
<thead>
<tr>
<th>Processes (What)</th>
<th>Methods (How)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Analysis</td>
<td>Architecture</td>
</tr>
<tr>
<td>Safety Requirements</td>
<td>Integrity (SIL/ASIL)</td>
</tr>
<tr>
<td>Management of Functional Safety</td>
<td></td>
</tr>
</tbody>
</table>

SIL = Safety Integrity Level
ASIL = Automotive SIL
Maturity Models & Functional Safety Standards

How they differ

<table>
<thead>
<tr>
<th>Maturity Models</th>
<th>Functional Safety Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Focus on software development, including systems</td>
<td>• Focus on development of safety-related systems, especially hardware characteristics</td>
</tr>
<tr>
<td>• Change management approach (capability levels)</td>
<td>• Capability for development of safety-related systems</td>
</tr>
<tr>
<td>• Approach to harmonize rating criteria, assessment method and to achieve comparability</td>
<td>• Context dependent assessment method and criteria are dominating</td>
</tr>
<tr>
<td>• Result is a certificate for process maturity</td>
<td>• Result is an expertise for a product</td>
</tr>
<tr>
<td>• Objective is efficient and repeatable development of any product or service</td>
<td>• Objective is capability to develop certain products with calculable risk</td>
</tr>
<tr>
<td>• Motivation for compliance is benefit</td>
<td>• Motivation is product liability</td>
</tr>
<tr>
<td>• Target level depends on business goals</td>
<td>• Target level depends on hazard analysis</td>
</tr>
<tr>
<td>• Give notation, requirements, guidance, best practice</td>
<td>• Give notation, requirements and some examples</td>
</tr>
<tr>
<td>• Do not require certain methods (“what”)</td>
<td>• Require certain methods (“how”) and characteristics (e.g. SFF)</td>
</tr>
</tbody>
</table>

Process Assessments and Safety Assessments

Comparison

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Process Assessment</th>
<th>Safety Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger</td>
<td>Before a project starts (supplier selection), early in a project, milestone or severe problems</td>
<td>Incremental after project start and at product release</td>
</tr>
<tr>
<td>Purpose</td>
<td>Capability determination or process improvement</td>
<td>Judge functional safety achieved</td>
</tr>
<tr>
<td>Qualification of the assessor</td>
<td>Automotive SPICE® PAM, assessment process</td>
<td>All elements of the safety standard</td>
</tr>
<tr>
<td>Model</td>
<td>Automotive SPICE®</td>
<td>Safety Standard IEC 61508/ISO/DIS 26262</td>
</tr>
<tr>
<td>Criteria</td>
<td>Process attributes, capability levels</td>
<td>Requirements of the standard</td>
</tr>
<tr>
<td>Rating scale</td>
<td>N, P, L, F</td>
<td>Not defined. Overall: Accepted/Rejected</td>
</tr>
<tr>
<td>Frequency</td>
<td>Often at most once per project</td>
<td>At least once before product release. Typically incrementally.</td>
</tr>
<tr>
<td>Scope split</td>
<td>Typically only HIS scope in Automotive. Individual processes possible. Only up to capability level x.</td>
<td>Phases, work products, subsystems, technology (system, hardware, software)</td>
</tr>
<tr>
<td>Information</td>
<td>Process capability, maturity of development processes</td>
<td>Assessor judgment whether the residual risk is low enough</td>
</tr>
</tbody>
</table>
Which Model and which Safety Standard?
Assumptions and context for this presentation

- Application context is primarily embedded E/E Automotive systems
- Typically: ECU (Electronic Control Unit) with connected sensors and actuators

Maturity Model:
- Automotive SPICE® PAM 2.5

Functional Safety Standard:
- ISO/DIS 26262

➢ Clearly identify model(s) and standard(s) according to business needs

---

ISO/IEC 15504 Processes

Automotive SPICE® & ISO/IEC 15504-5

- **Engineering Process Group (ENG)**
  - ENG.1 Requirements elicitation
  - ENG.2 System requirements analysis
  - ENG.3 System architectural design
  - ENG.4 Software requirements analysis
  - ENG.5 Software design
  - ENG.6 Software construction
  - ENG.7 Software integration
  - ENG.8 Software testing
  - ENG.9 System integration
  - ENG.10 System testing
  - ENG.11 Software installation
  - ENG.12 Software and system maintenance

- **Management Process Group (MAN)**
  - MAN.1 Organizational alignment
  - MAN.2 Organization management
  - MAN.3 Project management
  - MAN.4 Quality management
  - MAN.5 Risk management
  - MAN.6 Measurement

- **Supply Process Group (SPL)**
  - SPL.1 Supplier tendering
  - SPL.2 Product release
  - SPL.3 Product acceptance support

- **Resource & Infrastructure Process Group (RIN)**
  - RIN.1 Human resource management
  - RIN.2 Training
  - RIN.3 Knowledge management
  - RIN.4 Infrastructure

- **Operation Process Group (OPE)**
  - OPE.1 Operational use
  - OPE.2 Customer support

- **Process Improvement Process Group (PIM)**
  - PIM.1 Process establishment
  - PIM.2 Process assessment
  - PIM.3 Process improvement

- **Reuse Process Group (REU)**
  - REU.1 Asset management
  - REU.2 Reuse program management
  - REU.3 Domain engineering

- **Supporting Process Group (SUP)**
  - SUP.1 Quality assurance
  - SUP.2 Verification
  - SUP.3 Validation
  - SUP.4 Joint review
  - SUP.5 Audit
  - SUP.6 Product evaluation
  - SUP.7 Documentation
  - SUP.8 Configuration management
  - SUP.9 Problem resolution management
  - SUP.10 Change request management

Automotive SPICE® is a registered trademark of the Verband der Automobilindustrie e.V. (VDA).
# ISO/DIS 26262 Overview

## 1. Vocabulary

## 2. Management of functional safety
- 2.5 Overall safety management
- 2.6 Safety management during item development
- 2.7 Safety management after release for production

## 3. Concept phase
- 3.5 Item definition
- 3.6 Initiation of the safety lifecycle
- 3.7 Hazard analysis and risk assessment
- 3.8 Functional safety concept

## 4. Product development: system level
- 4.5 Initiation of product development at the system level
- 4.6 Specification of the technical safety requirements
- 4.7 System design
- 4.8 Item integration & testing
- 4.11 Release for production
- 4.10 Safety assessment
- 4.9 Safety validation

## 5. Product development: hardware level
- 5.5 Initiation of product development at the hardware level
- 5.6 Specification of hardware safety requirements
- 5.7 Hardware design
- 5.8 Hardware arch. metrics
- 5.9 Evaluation of violation of the safety goals
- 5.10 HW integration & testing
- 5.11 Vfication of software safety requirements

## 6. Product development: software level
- 6.5 Initiation of product development at the software level
- 6.6 Spec. of SW safety requirements
- 6.7 Software arch. design
- 6.8 SW unit design & implem.
- 6.9 Software unit testing
- 6.10 Software integration & testing
- 6.11 Verification of software safety requirements

## 7. Production and operation
- 7.5 Production
- 7.6 Operation, service (maintenance and repair), and decommissioning

## 8. Supporting processes
- 8.5 Interfaces within distributed development
- 8.7 Configuration management
- 8.8 Change management
- 8.9 Verification
- 8.10 Documentation
- 8.11 Qualification of SW tools
- 8.12 Qualification of SW components
- 8.13 Qualify. Of HW components
- 8.14 Proven in use argument

## 9. ASIL-oriented and safety-oriented analyses
- 9.5 Requirements decomposition with respect to ASIL tailoring
- 9.6 Criteria for coexistence of elements
- 9.7 Analysis of dependent failures
- 9.8 Safety analyses

## 10. Guideline (informative)

---

### Standards related to Functional Safety

**Derived from the generic standard**

[Diagram showing various standards such as ISO/DIS 26262, DO-178B, IEC 50156, EN 5012x, IEC 61508, IEC 61513, IEC 60335, IEC 60601, IEC 62061, and DO-178B.]
Relationship between ISO/DIS 26262 and Automotive SPICE

What means „SPICE-Compliance“? For the purpose of this presentation

• Maturity (typically) is different for different processes
• Maturity/capability may vary from project to project and may vary on organizational level
• Maturity may be unknown

➢ What needs to be changed/added/improved for functional safety depends on the maturity
• Do we need to know the Automotive SPICE maturity/capability?
  → Discussion
**Relationship Automotive SPICE - ISO/DIS 26262**

**What is supported?**

- **SPICE**: If compliant
- **ISO 26262**: ?

Suppose we have a CMMI or SPICE compliant process landscape. Which phases of the safety lifecycle and which clauses of the safety standard ISO/DIS 26262 then already have a good support? Expressed in a different way: Which requirements of the safety standards ask for little process changes or extension in order to become compliant?

---

**What is missing?**

- **SPICE**: If compliant
- **ISO 26262**: ?

Suppose we have a CMMI or SPICE compliant process landscape. Which phases of the safety lifecycle and which clauses of the safety standard ISO/DIS 26262 then will not be fulfilled? Expressed in a different way: Which requirements of the safety standards are missing and need explicit addition in the process landscape in order to become compliant?
### Notation

Within the following slides the phases and requirements of ISO/DIS 26262 are marked as follows:

- **Strong support** of this requirement by using processes designed to fulfill Automotive SPICE® Level 2/3 requirements
- **Medium support** by Automotive SPICE® Level 2/3 processes
- No or very **weak support** by Automotive SPICE® Level 2/3 processes

---

### SPICE and CMMI Support for ISO/DIS 26262

<table>
<thead>
<tr>
<th>1. Vocabulary</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-5 Overall safety management</td>
</tr>
<tr>
<td>3-6 Safety management during item development</td>
</tr>
<tr>
<td>3-7 Safety management after release for production</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. Management of functional safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-5 Item definition</td>
</tr>
<tr>
<td>3-6 Initiation of the safety lifecycle</td>
</tr>
<tr>
<td>3-7 Hazard analysis and risk assessment</td>
</tr>
<tr>
<td>3-8 Functional safety concept</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Concept phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5 Initiation of product development at the system level</td>
</tr>
<tr>
<td>4.6 Specification of the technical safety requirements</td>
</tr>
<tr>
<td>4.7 System design</td>
</tr>
<tr>
<td>4.8 Item integration &amp; testing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. Product development: system level</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5 Initiation of product development at the hardware level</td>
</tr>
<tr>
<td>5.6 Specification of hardware safety requirements</td>
</tr>
<tr>
<td>5.7 Hardware design</td>
</tr>
<tr>
<td>5.8 Hardware arch. metrics</td>
</tr>
<tr>
<td>5.9 Evaluation of violation of the safety goals</td>
</tr>
<tr>
<td>5.10 HW integration &amp; testing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5. Product development: hardware level</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5 Initiation of product development at the software level</td>
</tr>
<tr>
<td>6.6 Spec. of SW safety requirement</td>
</tr>
<tr>
<td>6.7 Software architectural design</td>
</tr>
<tr>
<td>6.8 SW unit design &amp; implementation</td>
</tr>
<tr>
<td>6.9 Software unit testing</td>
</tr>
<tr>
<td>6.10 Software integration &amp; testing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. Product development: software level</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5 Verification of software safety requirements</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. Production and operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5 Production</td>
</tr>
<tr>
<td>7.6 Operation, service (maintenance and repair), and decommissioning</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. Support processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8- 5 Interfaces within distributed development s</td>
</tr>
<tr>
<td>8- 7 Configuration management</td>
</tr>
<tr>
<td>8- 8 Change management</td>
</tr>
<tr>
<td>8- 9 Vartification</td>
</tr>
<tr>
<td>8-10 Documentation</td>
</tr>
<tr>
<td>8-11 Qualification of SW tools</td>
</tr>
<tr>
<td>8-12 Qualific. of SW components</td>
</tr>
<tr>
<td>8-13 Qualific. Of HW components</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9. ASIL-oriented and safety-oriented analyses</th>
</tr>
</thead>
<tbody>
<tr>
<td>9-5 Requirements decomposition with respect to ASIL tailoring</td>
</tr>
<tr>
<td>9-6 Criteria for coexistence of elements</td>
</tr>
<tr>
<td>9-7 Analysis of dependant failures</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10. Guideline (informative)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong support</td>
</tr>
<tr>
<td>Medium Support</td>
</tr>
<tr>
<td>Weak support</td>
</tr>
</tbody>
</table>
How much work to become compliant?
Areas with a lot of effort

? Where there is little support by Automotive SPICE there is more to do than where there is strong support.

- This statement does not help a lot. Typical areas with much additional effort:
  - Process improvement to achieve capability of developing safety-related products, including training/qualification
  - Functional and technical safety concept (design for safety)
  - Safety analyses (H&R, FTA, quantitative FMEA, hardware metrics, dependent failures)
  - Additional hardware components (sensors, processor, …)
  - Additional software for fault detection and control (3-level SW architecture)
  - Applying necessary test methods in a controlled way (fault injection, coverage, repetition after change, traceability of tests, …)
  - Qualification of tools and of components
  - Safety case including all the argumentation
  - Field monitoring process
How much work to become compliant?
Areas with limited additional effort for a mature organization

- Project management: Add activities, roles, work products, project effort and duration, assessment
- Configuration management: Add work products. Strict application.
- Change management: Strict application necessary
- Requirements analysis: Some additional safety requirements and attributes
- Software construction: More peer reviews and use of analysis tools

Relationship Automotive SPICE - ISO/DIS 26262
What is necessary?

In case compliance with ISO/DIS 26262 is required which processes, which practices and which work products are specifically necessary? Expressed in a different way: Which elements of SPICE or CMMI should specifically be emphasized? Which elements are important and which ones are not?
Automotive SPICE® Necessity for Functional Safety

Necessary Automotive SPICE® Capability Levels vary from 0 to 3. Formally no Capability Level necessary for Functional Safety. Recommendation from Functional Safety point of view only.

How to systematically identify what to change?

- Unidirectional mapping from Automotive SPICE to the (organization’s) standard process assumed
- Bidirectional mapping between ISO/DIS 26262 and Automotive SPICE useful for transparency of overlapping
- Gap analysis/conformity check of the standard process against the requirements of ISO/DIS 26262
- Maintain (at least) a unidirectional mapping from Automotive SPICE AND ISO/DIS 26262 to the standard process
Gap Analysis
Example / Extract / Tool

ISO/IEC 26262

<table>
<thead>
<tr>
<th>ClassNo.</th>
<th>Topic</th>
<th>Work Prod.</th>
<th>Table</th>
<th>Question</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.5.4</td>
<td>The work products referenced in the safety case:</td>
<td></td>
<td></td>
<td></td>
<td>— shall be subject to configuration and change management, in accordance with ISO°26262-8, Clause°7 and Clause°8, starting from the phase: product development at system level (see ISO°26262-4); and — shall be documented, in accordance with ISO°26262-8, Clause°50.</td>
</tr>
<tr>
<td>6.4.6.1</td>
<td>The confirmation measures shall be planned.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4.6.2</td>
<td>The confirmation measures, as specified in Table°1, shall be performed during the item development, including the following: a) the confirmation reviews; b) applies to ASIL (B), C, and D: Audit of functional safety processes; and c) applies to ASIL (B), C, and D: Assessment of functional safety, in accordance with 6.4.6.7.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Work Products of ISO/DIS 26262
How to implement in Automotive SPICE context (1/10)

<table>
<thead>
<tr>
<th>ISO/DIS 26262 Clause</th>
<th>Work Product</th>
<th>How to Implement it? Where? (Proposals, Ideas)</th>
<th>Association with Automotive SPICE process</th>
<th>Association with Automotive SPICE work products</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.1 Organization specific rules and processes for functional safety</td>
<td>Change policy. Update processes.</td>
<td>PD processes</td>
<td>Mission statement, vision, goals, process description, process repository.</td>
<td></td>
</tr>
<tr>
<td>5.5.2 Evidence that the persons assigned to carry out activities provided by ISO/DIS26262 have a sufficient level of skills, competences and qualification</td>
<td>Extend organisational training program</td>
<td></td>
<td>Personnel policy, training material, training plan.</td>
<td></td>
</tr>
<tr>
<td>5.5.3 Evidence of an operational E/E quality management system, conforming to the requirements of this part of ISO/DIS26262</td>
<td>Include functional safety criteria in QM activities. Update checklists. Maintain QM system certification.</td>
<td></td>
<td>Quality policy, quality manual, quality plan, quality criteria, review plan, quality record, review record.</td>
<td></td>
</tr>
<tr>
<td>5.5.3 Evidence of an operational E/E quality management system, conforming to the requirements of this part of ISO/DIS26262</td>
<td>Include functional safety criteria in QM activities. Update checklists. Maintain QM system certification.</td>
<td></td>
<td>Quality policy, quality manual, quality plan, quality criteria, review plan, quality record, review record.</td>
<td></td>
</tr>
<tr>
<td>5.5.3 Evidence of an operational E/E quality management system, conforming to the requirements of this part of ISO/DIS26262</td>
<td>Include functional safety criteria in QM activities. Update checklists. Maintain QM system certification.</td>
<td></td>
<td>Quality policy, quality manual, quality plan, quality criteria, review plan, quality record, review record.</td>
<td></td>
</tr>
<tr>
<td>6.5.1 Safety plan</td>
<td>Maintain separate plan or include in project plan</td>
<td></td>
<td>Project plan, project management plan, risk management plan, quality management plan, schedule, risk mitigation plan.</td>
<td></td>
</tr>
<tr>
<td>6.5.2 Overall project plan (refined)</td>
<td>Maintain project plan</td>
<td></td>
<td>Project plan, project management plan, risk management plan, quality management plan, schedule, risk mitigation plan.</td>
<td></td>
</tr>
<tr>
<td>6.5.3 Safety case</td>
<td>Collect references to evidence. Separate document with references and argumentation.</td>
<td></td>
<td>Verification results, quality record, audit report, assessment report.</td>
<td></td>
</tr>
<tr>
<td>6.5.4 Results of confirmation measures</td>
<td>Collect reports of confirmation measures. Part of the safety case.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5.5 Confirmation plan</td>
<td>Maintain separate plan or include in confirmation plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5.6 Functional safety assessment plan</td>
<td>Maintain separate plan or include in confirmation plan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.5 Evidence of a field monitoring process</td>
<td>Collect evidence until decommissioning according to separate monitoring process requirements</td>
<td></td>
<td>Field measure</td>
<td></td>
</tr>
</tbody>
</table>
Management of Functional Safety
Requirements from ISO/DIS 26262 part 2

- Overall project independent safety management
  - Definition of a safety policy and a safety strategy
  - Quality management system shall be in place
  - Company specific rules to be established
  - Tools, templates, data bases etc. to be provided
  - Lessons Learned passed on to subsequent projects
  - Safety training for involved persons
  - Decision on which phases of the safety lifecycle are to be carried out
  - Allocation of safety responsibility and duties for all safety related activities

- Project specific safety management
  - Create and maintain safety plan
  - Report safety findings to relevant management
  - Results of all activities to be documented
  - Planning of verification and validation activities
  - Determine level of independence for confirmation activities
  - Maintain a safety case
  - Define rules for safety management after start of production (SOP)
Development of Safety-related Systems
The Role of the Manager

- To be aware of its own responsibility and the risk
- Responsibility to establish a safety culture
- To establish requirements
- To clarify the integration of the functional safety process into the development process
- To allocate responsibility
- To establish positions and provide resources
- To take care of employees' training
- To request reports
- To actively observe the implementation

Work Products of ISO/DIS 26262
How to implement in Automotive SPICE context (2/10)
### Work Products of ISO/DIS 26262
#### How to implement in Automotive SPICE context (3/10)

<table>
<thead>
<tr>
<th>ISO/DIS 26262 Clause</th>
<th>Work Product</th>
<th>How to Implement?</th>
<th>Association with Automotive SPICE process</th>
<th>Association with Automotive SPICE work products</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Initiation of product development at the hardware level</td>
<td>5.5.2 Safety plan (refined)</td>
<td>Maintain separate plan</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td>6. Specification of hardware safety requirements</td>
<td>6.5.1 Hardware safety requirements specification</td>
<td>Separate additional activity</td>
<td>EN9.2 System requirements &amp; functional safety analysis</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>6.5.2 Hardware architectural metric requirements</td>
<td>Separate additional activity</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>6.5.3 Random hardware failure requirements</td>
<td>Separate additional activity</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>6.5.4 Hardware/software interface specification</td>
<td>Separate additional activity</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>6.5.5 Hardware safety requirements verification report</td>
<td>Update plan</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td>7. Hardware design</td>
<td>7.5.1 Hardware design specification</td>
<td>Maintain a hardware design</td>
<td>EN9.2 System architectural design</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>7.5.2 Hardware safety analysis report</td>
<td>Perform dedicated safety analyses (e.g. FTA, FMEA)</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>7.5.3 Hardware design verification report</td>
<td>Perform formal review and provide review report</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td>8. Hardware architectural metrics</td>
<td>8.5.1 Assessment of the effectiveness of the system architecture to cope with the hardware random failures</td>
<td>Perform dedicated assessment of hardware architectural metrics and provide report</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>8.5.2 Review report of assessment of the effectiveness of the system architecture to cope with the hardware random failures</td>
<td>Perform formal review and provide review report</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>8.5.3 Specification of dedicated metrics</td>
<td>Specification of dedicated metrics to be included in stated documents, depending on the measure</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>8.5.4 Review report of evaluation of the safety goal due to random HW failures</td>
<td>Perform formal review and provide review report</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>8.5.5 Hardware integration and verification report</td>
<td>Perform hardware integration and verification including the methods and tools required and document performance carefully</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
</tbody>
</table>

### Work Products of ISO/DIS 26262
#### How to implement in Automotive SPICE context (4/10)

<table>
<thead>
<tr>
<th>ISO/DIS 26262 Clause</th>
<th>Work Product</th>
<th>How to Implement?</th>
<th>Association with Automotive SPICE process</th>
<th>Association with Automotive SPICE work products</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Initiation of product development at the hardware level</td>
<td>5.5.2 Safety plan (refined)</td>
<td>Maintain separate plan</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td>6. Specification of hardware safety requirements</td>
<td>6.5.1 Hardware safety requirements specification</td>
<td>Separate additional activity</td>
<td>EN9.2 System requirements &amp; functional safety analysis</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>6.5.2 Hardware architectural metric requirements</td>
<td>Separate additional activity</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>6.5.3 Random hardware failure requirements</td>
<td>Separate additional activity</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>6.5.4 Hardware/software interface specification</td>
<td>Separate additional activity</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>6.5.5 Hardware safety requirements verification report</td>
<td>Update plan</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td>7. Hardware design</td>
<td>7.5.1 Hardware design specification</td>
<td>Maintain a hardware design</td>
<td>EN9.2 System architectural design</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>7.5.2 Hardware safety analysis report</td>
<td>Perform dedicated safety analyses (e.g. FTA, FMEA) and provide report(s)</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>7.5.3 Hardware design verification report</td>
<td>Perform formal review and provide review report</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td>8. Hardware architectural metrics</td>
<td>8.5.1 Assessment of the effectiveness of the system architecture to cope with the hardware random failures</td>
<td>Perform dedicated assessment of hardware architectural metrics and provide report</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>8.5.2 Review report of assessment of the effectiveness of the system architecture to cope with the hardware random failures</td>
<td>Perform formal review and provide review report</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>8.5.3 Specification of dedicated metrics</td>
<td>Specification of dedicated metrics to be included in stated documents, depending on the measure</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>8.5.4 Review report of evaluation of the safety goal due to random HW failures</td>
<td>Perform formal review and provide review report</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
<tr>
<td></td>
<td>8.5.5 Hardware integration and verification report</td>
<td>Perform hardware integration and verification including the methods and tools required and document performance carefully</td>
<td>M8.2 Planning</td>
<td>M8.3 Product development at the hardware level</td>
</tr>
</tbody>
</table>
## Work Products of ISO/DIS 26262
### How to implement in Automotive SPICE context (5/10)

<table>
<thead>
<tr>
<th>ISO/DIS 26262 Clause</th>
<th>Work Product</th>
<th>How to implement it? Where?</th>
<th>Association with Automotive SPICE process</th>
<th>Association with Automotive SPICE work products</th>
</tr>
</thead>
<tbody>
<tr>
<td>5: Initiation of product development at the software level</td>
<td>5.5.1.1 Software unit design specification</td>
<td>Maintain a software unit design</td>
<td>ENGL5 Software design / BP6ff.</td>
<td>Software unit design criteria</td>
</tr>
<tr>
<td>5: Software design and implementation</td>
<td>5.5.2.1 Software verification plan (refined)</td>
<td>Update plan</td>
<td>ENGL6 Software verification plan (refined)</td>
<td>Software verification plan (refined)</td>
</tr>
<tr>
<td>5: Software design and implementation</td>
<td>5.5.3.1 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>5: Software design and implementation</td>
<td>5.5.4.1 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>5: Software design and implementation</td>
<td>5:5.5 Software design and implementation</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software design and implementation</td>
<td>Software design and implementation criteria</td>
</tr>
<tr>
<td>5: Software design and implementation</td>
<td>5.5.6 Software design and implementation</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software design and implementation</td>
<td>Software design and implementation criteria</td>
</tr>
<tr>
<td>5: Software design and implementation</td>
<td>5.5.7 Software design and implementation</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software design and implementation</td>
<td>Software design and implementation criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.1.1 Software unit design specification</td>
<td>Maintain a software unit design</td>
<td>ENGL5 Software design / BP6ff.</td>
<td>Software unit design criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.1.2 Software unit implementation</td>
<td>Implement software unit according to coding rules</td>
<td>ENGL6 Software unit implementation</td>
<td>Software unit implementation criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.1.3 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.1.4 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.2.1 Software verification plan (refined)</td>
<td>Update plan</td>
<td>ENGL6 Software verification plan (refined)</td>
<td>Software verification plan (refined)</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.2.2 Software verification plan (refined)</td>
<td>Update plan</td>
<td>ENGL6 Software verification plan (refined)</td>
<td>Software verification plan (refined)</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.2.3 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.2.4 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.3.1 Software unit design specification</td>
<td>Maintain a software unit design</td>
<td>ENGL5 Software design / BP6ff.</td>
<td>Software unit design criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.3.2 Software unit implementation</td>
<td>Implement software unit according to coding rules</td>
<td>ENGL6 Software unit implementation</td>
<td>Software unit implementation criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.3.3 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.3.4 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.4.1 Software unit design specification</td>
<td>Maintain a software unit design</td>
<td>ENGL5 Software design / BP6ff.</td>
<td>Software unit design criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.4.2 Software unit implementation</td>
<td>Implement software unit according to coding rules</td>
<td>ENGL6 Software unit implementation</td>
<td>Software unit implementation criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.4.3 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.4.4 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.5.1 Software unit design specification</td>
<td>Maintain a software unit design</td>
<td>ENGL5 Software design / BP6ff.</td>
<td>Software unit design criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.5.2 Software unit implementation</td>
<td>Implement software unit according to coding rules</td>
<td>ENGL6 Software unit implementation</td>
<td>Software unit implementation criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.5.3 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.5.4 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.6.1 Software unit design specification</td>
<td>Maintain a software unit design</td>
<td>ENGL5 Software design / BP6ff.</td>
<td>Software unit design criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.6.2 Software unit implementation</td>
<td>Implement software unit according to coding rules</td>
<td>ENGL6 Software unit implementation</td>
<td>Software unit implementation criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.6.3 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.6.4 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.7.1 Software unit design specification</td>
<td>Maintain a software unit design</td>
<td>ENGL5 Software design / BP6ff.</td>
<td>Software unit design criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.7.2 Software unit implementation</td>
<td>Implement software unit according to coding rules</td>
<td>ENGL6 Software unit implementation</td>
<td>Software unit implementation criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.7.3 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6:7.4 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.8.1 Software unit design specification</td>
<td>Maintain a software unit design</td>
<td>ENGL5 Software design / BP6ff.</td>
<td>Software unit design criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.8.2 Software unit implementation</td>
<td>Implement software unit according to coding rules</td>
<td>ENGL6 Software unit implementation</td>
<td>Software unit implementation criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.8.3 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6:8.4 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.9.1 Software unit design specification</td>
<td>Maintain a software unit design</td>
<td>ENGL5 Software design / BP6ff.</td>
<td>Software unit design criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.9.2 Software unit implementation</td>
<td>Implement software unit according to coding rules</td>
<td>ENGL6 Software unit implementation</td>
<td>Software unit implementation criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.9.3 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6:9.4 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.10.1 Software unit design specification</td>
<td>Maintain a software unit design</td>
<td>ENGL5 Software design / BP6ff.</td>
<td>Software unit design criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.10.2 Software unit implementation</td>
<td>Implement software unit according to coding rules</td>
<td>ENGL6 Software unit implementation</td>
<td>Software unit implementation criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.10.3 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6:10.4 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.11.1 Software unit design specification</td>
<td>Maintain a software unit design</td>
<td>ENGL5 Software design / BP6ff.</td>
<td>Software unit design criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.11.2 Software unit implementation</td>
<td>Implement software unit according to coding rules</td>
<td>ENGL6 Software unit implementation</td>
<td>Software unit implementation criteria</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6.11.3 Software verification report (refined)</td>
<td>Perform formal review and/or static analysis of software implementation and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
<tr>
<td>6: Product development software level</td>
<td>6:11.4 Software verification report (refined)</td>
<td>Perform dynamic analysis, achieve test coverage, and provide reports</td>
<td>ENGL6 Software verification report (refined)</td>
<td>Software verification results, review record</td>
</tr>
</tbody>
</table>

### 6. Product development software level

[continued from previous page: 6. Product development software level]
### Work Products of ISO/DIS 26262
#### How to implement in Automotive SPICE context (7/10)

<table>
<thead>
<tr>
<th>ISO/DIS 26262 Clause</th>
<th>Work Product</th>
<th>How to implement? Where? (Proposals, Ideas)</th>
<th>Association with Automotive SPICE process</th>
<th>Association with Automotive SPICE work products</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Production</td>
<td>5.5.1 Production plan (refined)</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>5.5.2 Production control plan (refined) including test plan</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>5.5.3 Documentation of performed control measures</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>5.5.4 If applicable, requirements on the product liability at system- or software development level</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>5.5.5 Assessment report for capability of the production process</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>5.5.6 Maintenance plan (refined)</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>5.5.7 Repair instructions</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>5.5.8 User manual</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>5.5.9 Instructions regarding field observations</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>5.5.10 If applicable, requirements concerning operation, maintenance and decommissioning at system-, hardware or software development level</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
</tbody>
</table>

#### Work Products of ISO/DIS 26262
#### How to implement in Automotive SPICE context (8/10)

<table>
<thead>
<tr>
<th>ISO/DIS 26262 Clause</th>
<th>Work Product</th>
<th>How to implement? Where? (Proposals, Ideas)</th>
<th>Association with Automotive SPICE process</th>
<th>Association with Automotive SPICE work products</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Interfaces within distributed developments</td>
<td>6.5.1 Supplier selection report</td>
<td>Perform systematic supplier selection including safety criteria and document decisions</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>6.5.2 Development Interface Agreement (DIA)</td>
<td>Develop, agree upon and maintain a DIA as appendix to the contract. See also ISO/DIS 26262-8, Annex B: DIA example</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>6.5.3 Supplier’s project plan</td>
<td>Supplier maintains separate but consistent plan</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>6.5.4 Supplier’s safety plan</td>
<td>Supplier maintains separate but consistent plan</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>6.5.5 Safety assessment report</td>
<td>Include safety assessments at supplier side in DIA, perform assessments and provide a report for each assessment</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>6. Specification and management of safety requirements</td>
<td>6.5.6 Safety plan (refined)</td>
<td>Include requirements concerning safety requirements in requirements analyses processes</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>7. Configuration management</td>
<td>7.5.1 Configuration management plan</td>
<td>Update configuration management process and plan with work products specific for functional safety</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>7.5.2 Change management plan</td>
<td>Apply change management to work products specific for functional safety</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>7.5.3 Change request</td>
<td>Selecting specific for functional safety</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>7.5.4 Impact analysis and the change request plan</td>
<td>Take care to include criteria specific to functional safety, make persons in charge of functional safety</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>7.5.5 Change report</td>
<td>Carefully document changes to baselines</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>8. Change management</td>
<td>8.5.1 Verification plan</td>
<td>Maintain separate plan or multiple plans. May be integrated with confirmation plan. May be integrated with test plans</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>8.5.2 Verification report</td>
<td>Separate specification for reviews (checklists, ...) and for tests (test specification, ...), include safety criteria</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>10.5.1 Document management plan</td>
<td>Include documents and information specific to functional safety in the documentation plan</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>10. Documentation</td>
<td>10.5.2 Documentation requirements</td>
<td>Ensure that specific requirements for the safety standard are met</td>
<td>TBD</td>
<td>TBD</td>
</tr>
</tbody>
</table>

---

8. Supporting processes to be continued next page ➤
### Work Products of ISO/DIS 26262
How to implement in Automotive SPICE context (9/10)

continued from previous page: 8. Supporting processes

<table>
<thead>
<tr>
<th>ISO/DIS 26262 Clause</th>
<th>Work Product</th>
<th>How to Implement? Where? (Proposals, Ideas)</th>
<th>Association with Automotive SPICE process</th>
<th>Association with Automotive SPICE work products</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.5.1 Software tool classification analysis</td>
<td>Update necessary attributes of safety requirements</td>
<td>(ESI.2 Reuse program management)</td>
<td>system architectural design, software architectural design</td>
<td></td>
</tr>
<tr>
<td>11.5.2 Software tool qualification plan</td>
<td>Update necessary attributes of safety requirements</td>
<td>(ESI.2 Reuse program management)</td>
<td>requirements specification</td>
<td></td>
</tr>
<tr>
<td>11.5.3 Software tool documentation</td>
<td>Maintain a tool concept.</td>
<td>(ESI.2 Reuse program management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.5.4 Software tool qualification report</td>
<td>Maintain a document for each tool classified TQL 2 or 4</td>
<td>(ESI.2 Reuse program management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.5.1 Software component documentation</td>
<td>Maintain a document for each qualified software component or a set of software components</td>
<td>(ESI.2 Reuse program management)</td>
<td>customer manual</td>
<td></td>
</tr>
<tr>
<td>12.5.2 Software component qualification report</td>
<td>Provide evidence of successful qualification. Report for each component or for a set of components. Take care of timely availability for the project.</td>
<td>(ESI.2 Reuse program management)</td>
<td>reuse evaluation report</td>
<td></td>
</tr>
<tr>
<td>12.5.3 Safety plan (initial)</td>
<td>Update plan</td>
<td>(ESI.2 Reuse program management)</td>
<td>reuse strategy, reuse plan</td>
<td></td>
</tr>
<tr>
<td>12.5.5 Safety plan (final)</td>
<td>Update plan</td>
<td>(ESI.2 Reuse program management)</td>
<td>reuse strategy, reuse plan</td>
<td></td>
</tr>
<tr>
<td>13.5.1 Qualification plan</td>
<td>Establish a qualification plan for one component or for a set of components.</td>
<td>(ESI.2 Reuse program management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.5.2 Hardware component testing plan</td>
<td>Establish a testing plan or integrate the plan with the qualification plan or the project plan or the hardware testing/verification plan</td>
<td>(ESI.2 Reuse program management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.5.3 Qualification report</td>
<td>Provide evidence of successful qualification. Report for each component or for a set of components. Take care of timely availability for the project.</td>
<td>(ESI.2 Reuse program management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.5.1 Proven in use credit</td>
<td>Maintain a proven in use argument including necessary attachments for each candidate mentioned in the safety plan.</td>
<td>(ESI.2 Reuse program management)</td>
<td>reuse proposal</td>
<td></td>
</tr>
<tr>
<td>14.5.2 Definition of a candidate for proven in use argument</td>
<td>Identify candidates early in the project or even better independent from projects on an organisational level. Maintain a proven in use argument including necessary attachments for each candidate mentioned in the safety plan.</td>
<td>(ESI.2 Reuse program management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.5.3 Proven in use argument</td>
<td>Provide the argument early in the project in order to know whether it is substantiated. Maintain a proven in use argument including necessary attachments for each candidate mentioned in the safety plan.</td>
<td>(ESI.2 Reuse program management)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Work Products of ISO/DIS 26262
How to implement in Automotive SPICE context (10/10)

<table>
<thead>
<tr>
<th>ISO/DIS 26262 Clause</th>
<th>Work Product</th>
<th>How to Implement? Where? (Proposals, Ideas)</th>
<th>Association with Automotive SPICE process</th>
<th>Association with Automotive SPICE work products</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.2 Update of ASIL as attribute of safety requirements and elements</td>
<td>Do consider this clause in all design activities for safety requirements. Include this information in existing work products system safety specification, hardware design specification and/or software architectural design specification.</td>
<td>(RU.4 Infrastructure)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.6.1 Results of application of coexistence criteria and elements</td>
<td>Do consider this clause each time breaking down a safety-related element into sub-elements. Include this information in the technical safety concept and/or design documents.</td>
<td>(R IN.4 Infrastructure)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5.1 Results of analyses of dependent failures</td>
<td>Perform analysis of dependent failures in combination with safety analyses according to clause 7. Include this information in the results of safety analyses.</td>
<td>(RU.2 Reuse program management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5.2 Change requests for confirmed dependent failures</td>
<td>Include change requests for confirmed dependent failures in the technical safety concept and/or design documents.</td>
<td>(RU.2 Reuse program management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5.3 Results of safety analyses</td>
<td>Perform safety analyses during concept and product development phase. Great variety in methods, scope and time points possible. For each safety analysis planned in the safety plan provide the analysis itself, change requests as far as necessary, and additional test cases.</td>
<td>(RU.2 Reuse program management)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Copyright 2010 KUGLER MAAG CIE GmbH
Page 39 – SPICE Upgrade for Functional Safety
Necessary Measures to Provide a Safe Product

<table>
<thead>
<tr>
<th>Process</th>
<th>Product</th>
</tr>
</thead>
</table>
| • Management awareness  
  • Mature processes, customer and supplier, e.g.  
  • Process management, Project management,  
  • Change management, Configuration management  
  • Documentation  
  • Quality management  
  • Managed safety lifecycle  
  • Safety analyses  
  • Qualified staff members  
  • Qualified tools  
  • Organizational safety management  
  • Project specific safety management, e.g. safety case  
  • Management of distributed development  | • Verification  
 • Tests  
 • Audits  
 • Validation  
 • Assessment of functional safety |
| • Qualified components  
 • Proven-in-use components  
 • Safety requirements  
 • Safety architecture  
 • Redundancy  
 • Metrics (HW, …) | • Safety mechanisms  
 • Fault detection |

To avoid  

To detect and to control  

How to Achieve Compliance with ISO/DIS 26262
Achieve Compliance with ISO/DIS 26262
Perform a process improvement program

• What is a typical standard way for complying with ISO/DIS 26262 and Automotive SPICE in a development organization?
  • Steps, phases
  • Milestones, outcomes
  • Sequence, duration
  • Organization

➢ Standard Process for Compliance

Program Interrelationship
Process Improvement and Safety Compliance

• Do not consider this as two isolated activities!
  • There is only one standard process in the organization and one defined process in each project
  • The same people are concerned
  • The same projects are concerned
  • Maturity models and standards for functional safety overlap

• Actively manage both “sources for change and improvement”
  • Change management is similar
  • Program organization should highly overlap at least
  • Programs can be sequential or overlapping
Standard Process for Compliance

Overview

<table>
<thead>
<tr>
<th>Year</th>
<th>X</th>
<th>X+1</th>
<th>X+2</th>
<th>X+3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Initialization</td>
<td>Delta Phase</td>
<td>Rollout</td>
<td>Institutionalization</td>
</tr>
<tr>
<td>• Definition of objectives</td>
<td>• Process Definition</td>
<td>• Rollout to projects according to plan</td>
<td>• Continuous changes to processes</td>
<td></td>
</tr>
<tr>
<td>• Gap analysis</td>
<td>• Piloting</td>
<td>• Quality assurance</td>
<td>• Improve further processes due to business needs and customer requirements</td>
<td></td>
</tr>
<tr>
<td>• Action planning</td>
<td>• Transition</td>
<td>• Feedback loop</td>
<td>• Periodic re-assessments</td>
<td></td>
</tr>
<tr>
<td>• Project organization</td>
<td>• Intermediate Assessments</td>
<td>• Change management</td>
<td>• Confirmation assessment</td>
<td></td>
</tr>
<tr>
<td>• Commitments for plans and organization</td>
<td></td>
<td>• Continuous changes to processes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Initialization

• Activities
  • Vision: Definition of objectives
  • Gap analysis. Combined: Related to functional safety and Automotive SPICE
  • Action planning
  • Establish improvement project organization
  • Intelligent selection of pilot projects and process groups to pilot
  • Achieve commitments for plans and organization

• Duration
  • 1 - 4 months, before any further specific activities

• Outcomes
  • Project plan committed
  • Steering committee working, process owner committed, project core team established, process action teams initialized
Standard Process for Compliance

Delta Phase

- **Activities**
  - Process Definition
    - Includes process elements like templates and checklists, ready for piloting
  - Piloting
    - Improvement and completion of processes including process elements
    - Intensive coaching of pilot projects
  - Transition
    - Plan the rollout phase, including training concept
    - Train the trainer
    - Rules for transition to changed processes
  - Intermediate assessments

- **Duration**
  - 6 to 12 months depending on target maturity level and size of the organization
  - Duration of process definition shorter than piloting
  - Activities may overlap and may be performed e.g. per process group

- **Outcomes**
  - Organizational standard process for the development organization
  - Training and coaching package for the organization

Standard Process for Compliance

Rollout

- **Activities**
  - Rollout of the processes to projects according to plan
  - Rollout not only to new projects. Rollout of relevant processes according to project phase.
  - Incremental rollout of parts of the process landscape usually
  - Quality assurance, feedback loop and change management for processes are active
  - Confirmation assessment

- **Duration**
  - 6 to 18 months
  - Overlap with delta phase for some processes

- **Outcomes**
  - Organization works according to improved processes
Standard Process for Compliance
Institutionalization

- Activities
  - Have a team active for managing continuous changes to processes
  - Improve further processes due to business needs and customer requirements
  - Periodic re-assessments of maturity

- Duration
  - Continuously

- Outcomes
  - Organization continuously monitors process performance and improves processes

Steps of a Compliance Program

- Inventory of existing processes, tools and practices (initial assessment, gap analysis)
- Definition and prioritization of measures to fill the gaps
- Planning
- Definition of revised processes
- Pilot projects incl. coaching
- Performance reviews, intermediate assessments, lessons learned
- Process definition rework, definition of tailoring guidelines
- Rollout incl. coaching, training, monitoring
- Confirmation assessment
- Institutionalizing phase: Continuous improvement
The Roadmap to Change

 Initialization
Planning & Contracting

Pilot Project 1
Pilot Project 2
Pilot Project 3
Pilot Project 4

Roll-Out Project k
Roll-Out Project j
Roll-Out Project y

Start-Up Phase
Piloting Phase
Roll-Out Phase (~ 60% - 80% coverage)

05/2005
09/2005
2006
03/2007
03/2008
09/2009

Level 2
Level 3

Official Appraisal
Intermediate Appraisal

© Copyright 2010 KUGLER MAAG CIE GmbH
Page 51 – SPICE Upgrade for Functional Safety

Standard Process for Compliance
Organization

Management Control Board

(Engineering) Process Group

Quality Assurance

Product Marketing
Sales
Manufacturing
Delivery

Advanced Product Concepts
Product Development

Results Successes & Failures
Performance Targets & Objectives

Compliance Verification

Ability Support

Business Units Core Processes

© Copyright 2010 KUGLER MAAG CIE GmbH
Page 52 – SPICE Upgrade for Functional Safety
Example: Organization Principle Bosch
Published on Safetronic 2009, Munich

### Safetronic 2009

#### Organisatorische Aufstellung (1)

- **RB Safety Control Board:** Verantwortliche für Zentralstellen- und Entwicklungsleitungen der Geschäftsbereiche
- **RB Safety Teams:** Vertreter der Geschäftsbereiche
- **Team ISO 26262:** Verantwortliche für die jeweiligen Normteile

#### Geschäftsbereiche, Zentralstellen und -abteilungen

- AE
- CC
- GS
- DS
- ... C

#### Ermittlung der Firmeninteressen

#### Diskussion der Normumsetzung

#### Expertenteams: Fachexperten in den Geschäftsbereichen

---

### Possible ISO 26262 Master Plan set-up

#### Safety Control Board:
- Focus: Strategy & Policy

#### Safety Team:
- Focus: Cross BU's

#### Expert Workshops

#### Team ISO 26262
- Focus: Standard

#### PM

---

**Project**

„Functional Safety ISO 26262“
Process Improvement and Safety Compliance
List of Process Action Teams (Proposal)

- Project Management
- Requirements Elicitation and Management
- Safety Analyses and Assessment
- System Architecture
- System Integration, Test, and Validation
- Software Architecture
- Software Implementation
- Software Test
- Hardware Architecture
- Quality Management
- Build Management and Configuration Management
- Problem and Change Request Management
- Tool Concept and Tool Qualification

Note: This is not a blueprint for all organizations. Case to case decision necessary depending on many factors.

Functional Safety Service Center in the Organization

Organizational units providing know-how and resources

- Hardware design
- Software design
- Test
- Quality
- FSSC: Functional Safety Service Center
What is a Functional Safety Service Center?

FSSC

- It is an organizational entity to systematically establish and manage functional safety
- It provides guidance, know-how and internal/external resources for getting started with safety activities (jump start with external know-how and resources)
- It provides training and qualification of project staff with respect to functional safety knowledge required to perform safety-related analysis, design and test activities
- It enables improving of standard processes on the organizational level to become compliant with safety standards
- It facilitates the transfer of external know-how into the organization
- It is an efficient job-aid for all safety-related activities throughout the complete lifecycle

FSSC Benefits

- Culture of safe work
- Safe products
- Customer satisfaction
- Reduced rework
- Calculable product risk
- Optimized effort for process maturity (multi-model compliance)
- Process maturity with defined results
- Full compliance with safety-related standards such as IEC 61508 and ISO/DIS 26262
FSSC Services

The project side: Develop safe products

Planning functional safety in projects
- Sales support
- Supplier management
- Functional safety plan including
  - Analyses, design, and test for safety
  - Confirmation measures
  - Project safety process
- Safety know-how

Managing functional safety in projects
- Hazard and risk analysis
- Functional and technical safety concept
- Safety architecture
- Safety analyses (FTA, FMEDA, ...)
- Test support
- Reviews, audits, assessments
- Safety case

Establish functional safety competence
- Safety training
- Safety job aid workshop
- Design for functional safety
- Safety analyses training (H&A, FTA, FMEDA)
- Testing safety-related products
- Functional safety networking
- Qualified Project Safety Engineer (QFSE)

Managing functional safety for the Organization
- Safety process compliance check
- Provide organizational processes for safety
- Qualification of hard- and software components
- Qualification of software tools

The organizational side: Achieve functional safety capability

Roles
Affected by the FSSC

<table>
<thead>
<tr>
<th>Roles</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Existing</strong></td>
<td></td>
</tr>
<tr>
<td>Project Manager</td>
<td>Managing the project including safety aspects</td>
</tr>
<tr>
<td>Hardware Architect</td>
<td>Designing the hardware architecture for safety require</td>
</tr>
<tr>
<td>Software Architect</td>
<td>Designing the software architecture for safety require</td>
</tr>
<tr>
<td>Reviewer</td>
<td>Reviewing work products (e.g. safety concept, test plan)</td>
</tr>
<tr>
<td>Tester</td>
<td>Testing hardware/software systems with specific methods</td>
</tr>
<tr>
<td>Auditor</td>
<td>Checking implementation of functional safety processes</td>
</tr>
<tr>
<td><strong>New</strong></td>
<td></td>
</tr>
<tr>
<td>Functional Safety Manager</td>
<td>Managing functional safety on organization level</td>
</tr>
<tr>
<td>Project Safety Engineer</td>
<td>Planning and implementing safety activities in the project</td>
</tr>
<tr>
<td>Trainer</td>
<td>Training of project staff on safety standards &amp; methods</td>
</tr>
<tr>
<td>Safety Assessor</td>
<td>Checking the achievement of safety goals</td>
</tr>
</tbody>
</table>
Management of Functional Safety
Recommendations from practice (1)

Implement the role „Functional Safety Manager“
- Overall across projects
- Responsible for the definition of the functional safety process
- Definition of tools and resources
- Qualification of the development tools and libraries
- Coordination of audits across projects
- Safety management during the offer phase (up to the project kick-off)
- Safety management after development project closure (SOP)
- Provision of persons specifically qualified (e.g. auditors, assessors and for safety analyses)
- Leader of the Project Safety Engineers/Managers
- Reports to senior management

Management of Functional Safety
Recommendations from practice (2)

Implement the role „Project Safety Engineer / Manager“
- Project specific role
- Drives the safety related processes in the project
- Creates the safety plan
- Responsible for all functional safety work products
- Steers the safety related activities in the project
- Moderates analysis sessions or performs safety analyses
- Organizes reviews, audits and safety assessments
- Interface to the customer and to the suppliers for functional safety
- Maintains the safety case
- Reports to the Functional Safety Manager and to the Project Manager
FSSC Implementation
Activities and timeline

1. Functional safety introduction for management
2. Safety process gap analysis and action plan proposal
3. Define functional safety strategy for the organization
4. Set up a FSSC steering board
5. Approve functional safety strategy for the organization
6. Assign Functional Safety Manager
7. Define process tailoring guidelines
8. Train staff
9. Assign Project Safety Engineer
10. Set up safety planning for a customer project
11. Perform and support safety activities in the project as planned

FSSC Instruments

- Functional safety training modules
- Safety assessment workbench
- Safety analysis workbench
- Sample safe architectures
- Job aid for confirmation measures
- Functional safety process templates (process additions, work product templates, roles, glossary, ...)

© Copyright 2010 KUGLER MAAG CIE GmbH
Page 63 – SPICE Upgrade for Functional Safety
### Example: Hazard and Risk Analysis

<table>
<thead>
<tr>
<th>What</th>
<th>Performing hazard and risk analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Scheduling the workshop</td>
</tr>
<tr>
<td></td>
<td>• Preparing the input documents</td>
</tr>
<tr>
<td></td>
<td>• Performing the workshop</td>
</tr>
<tr>
<td></td>
<td>• Documenting the results</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who / Roles</th>
<th>Hardware Architect</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Software Architect</td>
</tr>
<tr>
<td></td>
<td>Functional Safety Manager (moderating)</td>
</tr>
<tr>
<td></td>
<td>Project Safety Engineer (preparing, documenting)</td>
</tr>
</tbody>
</table>

| When                  | Once in the concept phase of the customer project and at any change of the safety-related system as part of impact analysis |

<table>
<thead>
<tr>
<th>Input</th>
<th>H&amp;R templates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Scope definition (vehicle class, countries, customer requirements)</td>
</tr>
<tr>
<td></td>
<td>List of operating modes (e.g. power up, shut down, normal operation)</td>
</tr>
<tr>
<td></td>
<td>List of operating situations (weather, traffic situation etc.)</td>
</tr>
<tr>
<td></td>
<td>Catalogue of potential operating errors</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Result</th>
<th>Safety goals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Top level safety requirements</td>
</tr>
<tr>
<td></td>
<td>ASIL (Automotive Safety Integrity Level)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Effort / Duration</th>
<th>4 Person Days for preparing and documenting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 Days workshop (4 participants)</td>
</tr>
</tbody>
</table>

---

### Timeline for Functional Safety Compliance

- Compliance
Temporal Considerations
Compliance with Safety Standard(s)

- Necessary period for achieving compliance with ISO/DIS 26262 is comparable with improving by one maturity level:
  - A few years. It depends on …
  - No one does it in one step. Always in increments.
  - Important to begin! Make a plan with what to begin.
  - Beginning is urgent
    - Apply state-of-the-art techniques at the time of product release
    - ISO 26262 is continuously replacing IEC 61508 as state-of-the-art techniques for Automotive until 2011
    - Compliance is recommended/required for products sold
    - Development time is typically 3 years in Automotive

---

When to Begin? Example.
Introduction of ISO 26262 at a German OEM

![Diagram showing temporal considerations and ISO milestones for 2008 to 2015]

- **ISO-Milestones**
  - CD
  - DIS
  - IS

- **When to Begin**
  - 2008 (60 months before SOP)
  - 2009 (60 months before SOP)
  - 2011 (60 months before SOP)
Gap Analysis and Planning for a Project
Example: Proposal for work package

- **Activities**
  - Perform functional safety gap analysis for one project
  - Leading standard for the gap analysis is ISO/DIS 26262.
  - Expectations of Automotive SPICE (HIS scope) will be considered up to maturity level 2.
  - Define improvement infrastructure
  - Plan process improvement activities for the project

- **Duration**
  - Two consecutive weeks onsite: 1 week gap analysis, 1 week planning

- **Outcomes**
  - Analysis report and project plan
  - Plan for continuous consulting and intermediate performance checks
Gap Analysis and Planning for a Project

Effort indication

- Team
  - Consulting
    - 12 days effort for functional safety and A-SPICE expert
  - Organization's team member
    - 10 days effort for the team member
    - Development organization member with good standing

Perform ISO/DIS 26262 Gap Analysis
With Automotive SPICE considerations

Objectives
- To identify the gaps between the requirements of the safety standard ISO/DIS 26262 and actual planning and application of processes, methods, and techniques in a project. To identify the gaps with respect to infrastructure, organizational structures for safety and established safety culture. The main focus of the analysis is placed on ISO/DIS 26262 part 2, 4, 5, 6, and the supporting processes from part 8 and 9.
- Consider Automotive SPICE standard requirements for gap analysis and definition of improvement measures

Content
1. Short introduction into relevant project's documents such as process descriptions and project handbook
   - Product architecture and specification
   - Functional and technical safety concepts
   - Safety plan and project plan
   - Quality plan
   - Test- and verification plans, test specifications
   - Verification and test results
2. Get familiar with the documents and plan the systematic gap analysis (planning of joint working sessions for the analysis)
3. Analyze documents and check if processes, methods, infrastructure, and organizational structures are adequate to fulfill the general requirements (planning, configuration management, documentation etc.)
   - to fulfill specific requirements according to the required ASIL
   - regarding the system and SW architecture and the diagnostics.
4. Check whether tools in use reflect the state of practice, with particular attention to collecting evidences for the safety case
5. Perform interviews with process and product experts to clarify questions regarding the analyzed documents and to obtain additional information not contained in the documentation
6. Derive measures to close the gaps; some measures address Automotive SPICE-related issues
7. Review the organizational set-up suitable for maintaining a functional safety culture; perform short (1h) interviews with key stakeholders, like upper management
8. Compile the analysis report including proposed measures and suggestions for tools and their integration
9. Results presentation & discussion of measures and next steps

Customer Obligations
- The organization provides relevant documents as specified in “Content”
- Safety Manager and Safety Engineer, Project Manager and Quality Engineers (System and SW), Requirements Manager, Architects, Developers, Testers, are available for interviews and to provide information on the project's safety concept
SPICE Work Product 10-00 Process Description
Small differences for functional safety

Automotive SPICE:
• A detailed description of the process/procedure which includes:
  • tailoring of the standard process (if applicable)
  • purpose of the process
  • outcomes of the process
  • task and activities to be performed and ordering of tasks
  • critical dependencies between task activities
  • expected time required to execute task
  • input/output work products
  • links between input and outputs work products
• Identifies process entry and exit criteria
• Identifies internal and external interfaces to the process
• Identifies process measures
• Identifies quality expectations
• Identifies functional roles and responsibilities
• Approved by authorised personnel

Functional Safety:
• Additionally:
  • Methods how to do it
  • Dependence from ASIL
  • Tool to be used (qualified)
  • Independence for confirmation measures
  • Mandatory activities (e.g. H&R, confirmation measures)
  • Mandatory work product attributes (e.g. for functional safety requirements)
• Not all SPICE characteristics are required for functional safety, e.g.
  • expected time required to execute task
  • process measures

What to Change in Standard Process?
Implement change in all kinds of elements of processes

• Changed, additional, deleted elements
• Variants according to ASIL

• Lifecycle
• Process
• Activity in a process
• Work product
• Template
• Checklist
• Method
• Tool
• Attribute
• Role
## Confirmation Measures

### Reviews, Audits and Assessments in the Lifecycle

<table>
<thead>
<tr>
<th>Safety Lifecycle</th>
<th>Concept phase</th>
<th>Product Development</th>
<th>Production, Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Project Start</td>
<td>Start Product</td>
<td>SOP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Development</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sample</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sample</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>End of Decommissioning</td>
</tr>
</tbody>
</table>

### Reviews
- Hazard analysis, risk assessment, safety goals
  - Safety plan
  - Integration and test plan
  - Validation plan
  - Safety analyses
  - V&V test cases
  - V&V tests
  - V&V tests

### Audits
- Project independent
- After initiation of product development
  - After initiation of product development at hardware level
  - After initiation of product development at software level
  - After a major sample
  - After a major sample
- At product release

### Assessments of functional safety
- Intermediate

---

© Copyright 2010 KUGLER MAAG CIE GmbH
Page 76 – SPICE Upgrade for Functional Safety
### Evaluations in the Safety Lifecycle

<table>
<thead>
<tr>
<th>Safety Lifecycle</th>
<th>Project independent</th>
<th>Concept phase</th>
<th>Product Development</th>
<th>Production, Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification</td>
<td>Walkthrough</td>
<td>Review</td>
<td>Inspection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Testing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety Validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- ● Activity specific for A-SPICE
- ○ Activity specific for functional safety
- □ Joint activity
- ○ Optional activity

### ISO/DIS 26262-2 Confirmation Measures

#### Table 2 — Types of confirmation measures for ensuring functional safety

<table>
<thead>
<tr>
<th>Subject</th>
<th>Functional safety audit</th>
<th>Confirmation review</th>
<th>Functional safety assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Implementation of the processes required for functional safety</td>
<td>Work product</td>
<td>Item as described in the item definition (see ISO<em>26262-3, Clause</em>5)</td>
</tr>
<tr>
<td>Result</td>
<td>Audit report*</td>
<td>Confirmation review report*</td>
<td>Assessment report on functional safety of the item</td>
</tr>
<tr>
<td>Responsibility of the Auditor/Reviewer/Safety Assessor</td>
<td>Adequate evaluation of the processes against the definition of the activity, referenced or listed in the safety plan.</td>
<td>Adequate evaluation of the compliance of the work product with the respective requirements of ISO*26202</td>
<td>Adequate evaluation of the achieved functional safety level</td>
</tr>
<tr>
<td>Timing during lifecycle</td>
<td>During implementation of the required processes</td>
<td>After completion of the corresponding safety activity Completion before product release</td>
<td>Progressively during development, or in a single block Completion before product release</td>
</tr>
<tr>
<td>Scope and depth</td>
<td>Determined by the auditor</td>
<td>Planned prior to the review, in accordance with the safety plan</td>
<td>Review of processes and safety measures required for functional safety</td>
</tr>
</tbody>
</table>

* Can be included in a functional safety assessment report
Two Interesting Notes
ISO/DIS 26262-2, clause 6.4.6.3

NOTE 1 on combining a SPICE assessment with a functional safety assessment
- If the functional safety assessment is performed by a qualified SPICE assessor, then the functional safety audit and a SPICE assessment can be performed simultaneously. There is sufficient commonality in content between ISO 26262 and SPICE to allow synchronization of the planning, and execution of, for some supporting processes. Otherwise, if synchronized, the certified SPICE assessor can provide feedback to the safety assessor.

NOTE 2 on compliance of process definitions with SPICE and ISO 26262
- An organization’s process definitions can address multiple standards at the same time, e.g., functional safety requirements of ISO 26262 and SPICE. This might help to avoid duplication of work or process inconsistencies. In those cases, organization specific reference lists of process references to ISO 26262 requirements and to SPICE base practices can be provided.

Example: Confirmation Measures Bosch
Published on SPICE Days 2009, Stuttgart
Example: Assessement Methods Bosch
Published on SPICE Days 2009, Stuttgart

Success Factors for Achieving Functional Safety Capability
Comparable with Process Improvement Success Factors
Success is a Question of Culture

Safety culture
• There needs to be a culture for providing safe products
  • Safety Culture (ISO/DIS 26262-1, 1.104): Policy and strategy used within an organization to support the development, production, and operation of safety-related systems

Process culture
• There needs to be a culture to work in a systematic way according to constantly improving procedures

Some definitions of “culture”
• Culture is a collective programming of the mind that distinguishes the members of one group or category of people from another. (www.tamu.edu)
• Culture is a shared, learned, symbolic system of values, beliefs and attitudes that shapes and influences perception and behavior -- an abstract "mental blueprint" or "mental code." (www2.eou.edu)

Success Factors for Process Improvement

- Skills
- Incentives
- Resources
- Vision
- Improvement
- Commitment
- Communication/Change Mgmt.
- PI Program Management
- Culture
Consequences of missing Success Factors
They all are important

Management, Communication, and Culture

Health Check

Make a Health Check to determine whether your organization is likely to succeed
Cost Considerations

Functional Safety Capability
Effort / Cost on the Organizational Level

**Extension of documented processes** for functional safety (organizational level).
Assumed: CMMI/SPICE maturity „nearly“ 2; medium size organization
**200 person days** (process descriptions, utilities, piloting, …)

**Maintaining** functional safety capability on an organizational level.
Depends on the size of the organization.
For 50 – 100 developers in safety related development projects **one person in full time** (e.g. Functional Safety Manager)

- Additional roles, additional process elements, new and changed templates, tools, training, …
- Definition, piloting, rollout
- Much less effort for a mature organization
- KUGLER MAAG CIE experiences
Management of Functional Safety
Effort / Cost for a Project

• Effort for SIL / ASIL projects will increase when compared to non safety-related projects of the same complexity

<table>
<thead>
<tr>
<th>IEC 61508</th>
<th>ISO/DIS 26262</th>
<th>Effort Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A</td>
<td>15 - 25 %</td>
</tr>
<tr>
<td>2</td>
<td>B</td>
<td>20 - 40 %</td>
</tr>
<tr>
<td>3</td>
<td>C</td>
<td>30 – 60 %</td>
</tr>
<tr>
<td>3</td>
<td>D</td>
<td>50 – 100 %</td>
</tr>
</tbody>
</table>

Note:
• Estimation, not measured data
• Many factors heavily influence actual effort
• Clarify assumptions and requirements before making estimations

Summary

• Maturity models and standards for functional safety overlap
  • Some supporting, some missing, some required elements in Automotive SPICE
  • A process assessment is not an assessment of functional safety
  • Maintain a mapping from the maturity model and the functional safety standard to the standard process
• Safety measures need to be implemented
  • Product and process
  • To avoid, to detect and to control faults
• A program must be performed to achieve safety compliance
  • A gap analysis identifies what to do to achieve safety compliance
  • Change management is key for a success of this program
  • Cost of functional safety heavily vary depending on circumstances
  • An organizational unit is recommended to manage functional safety across projects (Functional Safety Service Center)
• It is urgent to achieve safety compliance because of product liability
Thank you for your participation!

Should you have any questions please do not hesitate to contact us ...

KUGLER MAAG CIE GmbH
Leibnizstraße 11
D-70806 Kornwestheim
Internet: www.kuglermaag.com
Tel. Office : +49 7154 - 807 210
Email: Safety@kuglermaag.com

Dr. Erwin Petry
Email: Erwin.Petry@kuglermaag.com
Mobile: +49 (0) 173-678 7337

Our Book about Functional Safety
(in German)

Can be ordered here: http://www.kuglermaag.de/webshop.html