Automotive SPICE® & ISO/CD 26262
Their Mutual Relationship

Dr. Erwin Petry

KUGLER MAAG CIE GmbH
Leibnizstraße 11 · D-70806 Kornwestheim
Mobil: +49 173 6787337
E-Mail: erwin.petry@kuglermaag.com · Internet: www.kuglermaag.com

Milan, June 04, 2009
Automotive SPIN Italia, www.automotive-spin.it

ISO/IEC 15504 Processes

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A ENG.1 Requirements elicitation</td>
<td>A MAN.1 Organizational alignment</td>
<td>A REU.1 Asset management</td>
</tr>
<tr>
<td>A ENG.2 System requirements analysis</td>
<td>A MAN.2 Organization management</td>
<td>A REU.2 Reuse program management</td>
</tr>
<tr>
<td>A ENG.3 System architectural design</td>
<td>A MAN.3 Project management</td>
<td>A REU.3 Domain engineering</td>
</tr>
<tr>
<td>A ENG.4 Software requirements analysis</td>
<td>A MAN.4 Quality management</td>
<td></td>
</tr>
<tr>
<td>A ENG.5 Software design</td>
<td>A MAN.5 Risk management</td>
<td></td>
</tr>
<tr>
<td>A ENG.6 Software construction</td>
<td>A MAN.6 Measurement</td>
<td></td>
</tr>
<tr>
<td>A ENG.7 Software integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A ENG.8 Software testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A ENG.9 System integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A ENG.10 System testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A ENG.11 Software installation</td>
<td>A SPL.1 Supplier tendering</td>
<td></td>
</tr>
<tr>
<td>A ENG.12 Software and system maintenance</td>
<td>A SPL.2 Product release</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A SPL.3 Product acceptance support</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Acquisition Process Group (ACQ)

| ACO.1 Acquisition preparation |
| ACO.2 Supplier selection |
| ACO.3 Contract agreement |
| ACO.4 Supplier monitoring |
| ACO.5 Customer acceptance |
| ACO.11 Technical requirements |
| ACO.12 Legal and administrative requirements |
| ACO.13 Project requirements |
| ACO.14 Request for proposals |
| ACO.15 Supplier qualification |

Supporting Process Group (SUP)

| A SUP.1 Quality assurance |
| A SUP.2 Verification |
| A SUP.3 Validation |
| A SUP.4 Joint review |
| A SUP.5 Audit |
| A SUP.6 Product evaluation |
| A SUP.7 Documentation |
| A SUP.8 Configuration management |
| A SUP.9 Problem resolution management |
| A SUP.10 Change request management |
| SUP.8 Configuration management |

HIS-Scope

not included in ISO/IEC 15504-5
ISO WD 26262 Overview (BL4)

ISO CD 26262 Safety Lifecycle

3.4 Item definition
3.5 Initiation safety lifecycle
3.6 Hazard/ risk analysis
3.7 Functional safety concept

4. Product development system level

5 HW level
6 SW level

4.10 Product release

7.4 Production
7.5 Operation, service

Planning
7.5
7.4
Operation
Product
Development
After
SOP

Comparison Lifecycle - Processes - QM

CMMI / SPICE processes support the implementation

<table>
<thead>
<tr>
<th>Safety Lifecycle</th>
<th>Concept phase</th>
<th>Product development</th>
<th>After SOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifecycle OEM</td>
<td>Safety requirements</td>
<td>Series Development</td>
<td>Production</td>
</tr>
<tr>
<td>Lifecycle Supplier</td>
<td>Advance Development</td>
<td>Development</td>
<td>Service</td>
</tr>
</tbody>
</table>

Support Processes

CMMI
- RM, SAM, PP, PMC, CM, ..

SPICE (HIS)
- MAN.3, ACQ.4, ENG.2-10, ...

QM
- ISO 9000:2000 / ISO 16949

Maturity Models & Functional Safety Standards
How they differ

**Maturity Models**
- Focus on software development, including systems
- Change management approach (capability levels)
- Approach to harmonize rating criteria, assessment method and to achieve comparability
- Result is a certificate for process maturity
- Objective is efficient and repeatable development of any product or service
- Motivation for compliance is benefit
- Target level depends on business goals
- Give notation, requirements, guidance, best practice
- Do not require certain methods (“what”)

**Functional Safety Standards**
- Focus on development of safety-related systems, especially hardware characteristics
- Capability for development of safety-related systems
- Context dependent assessment method and criteria are dominating
- Result is an expertise for a product
- Objective is capability to develop certain products with calculable risk
- Motivation is product liability
- Target level depends on hazard analysis
- Give notation, requirements and some examples
- Require certain methods (“how”) and characteristics (e.g. SFF)
Functional Safety and Maturity Models
They support each other

Requirements from IEC 61508 / ISO CD 26262

Risk Analysis
Safety Plan

Architecture Integrity (SIL/ASIL)

Management of Functional Safety

SIL = Safety Integrity Level
ASIL = Automotive SIL

Requirements from CMMI / Automotive SPICE

CMMI / A-SPICE e.g. Project Management, Configuration Management

Notation

Within the following slides the processes of Automotive SPICE are marked as follows:

- **Strong necessity** of this process for safety-related E/E/PE developments
- **Medium necessity** of this process for safety-related E/E/PE developments
- No or very **weak necessity** of this process for safety-related E/E/PE developments
Automotive SPICE Necessity for Functional Safety

The Acquisition Process Group (ACQ)
- ACQ.1 Acquisition preparation
- ACQ.2 Supplier selection
- ACQ.3 Contract agreement
- ACQ.4 Supplier monitoring
- ACQ.5 Customer acceptance
- ACQ.11 Technical requirements
- ACQ.12 Legal and administrative requirements
- ACQ.13 Project requirements
- ACQ.14 Request for proposals
- ACQ.15 Supplier qualification

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

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

The 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

Notation

Within the following slides the phases and requirements of IEC 61508 resp. ISO WD 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
Automotive SPICE Support for IEC 61508 E/E/PES Realization Phase

- **9.1** E/E/PES safety requirements specification
  - 9.1.1 Safety functions
  - 9.1.2 Safety integrity

- **9.2** Validation planning
- **9.3** Design and development
- **9.4** Integration
- **9.5** Operation and maintenance
- **9.6** Validation

Confirmation Measures

Reviews, Audits and Assessments in the Lifecycle

### Safety Lifecycle

- **Concept phase**
  - Project Start
  - Start Product Development

- **Product Development**
  - Sample
  - Sample
  - V&V-plan
  - V&V test cases
  - V&V test cases
  - V&V test cases
  - V&V tests
  - V&V tests
  - V&V tests

- **Production, Operation**
  - SOP
  - End of Decommissioning

### Reviews

- Hazard analysis, risk assessment, safety goals
  - Safety plan
  - Functional and technical safety requirements
  - Safety analyses
  - V&V test cases
  - V&V tests

- Qualification of parts and components
  - Safety case
  - Proof in use argument

### 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
  - After a major sample
  - At product release
  - During production and operation

### Assessments of functional safety

- Intermediate
  - At product release
Dependency Graph for Evaluation Methods

Analysis Safety analysis
Walkthrough Review Inspection
Quality management audit
Testing Validation
Audit Safety validation
Process assessment

A depends on A: B can profit from previous performance of A
B performance of A

Functional Safety Assessment
CMMI and SPICE context

CMMI and SPICE processes support safety assessments by providing reports and status information. It is however not their objective to judge on functional safety.
Backup

Automotive SPICE support for functional safety in more detail

Example:

Management of Functional Safety
Management of Functional Safety
Requirements from IEC 61508 (1)

- Ensure a culture of safe working
  - Definition of policies and strategies for achieving functional safety, communication of policies and strategies
- Identification of persons, departments, organisations responsible for
  - Carrying out the measures
  - Reviewing the results of the measures
- Definition of the safety lifecycle phases to be applied
  - System/ Hardware development
  - Software development
- Describe documentation rules considering
  - Structure of the documentation
  - Level of detail
  - Archiving of data and documents

Management of Functional Safety
Requirements from IEC 61508 (2)

- Definition of the measures to be performed and the related methods to be applied during implementation
  - Hazard and risk analysis
  - Functional safety assessment
  - Verification and validation activities
  - Organization specific interpretation of the requirements described in tables of the IEC 61508 part 2, part 3 and part 6
- Ensure involved parties are competent to carry out activities
  - Training of designers
  - Training of maintenance staff
  - Retraining at periodic intervals
Management of Functional Safety
Requirements from IEC 61508 (3)

• Definition of procedures for the analysis of hazardous incidents
• Definition of procedures and rules to ensure functional safety during the maintenance phase
• Specification of requirements for periodic functional safety audits
• Definition of procedures for initiating modifications to the safety related system
• Configuration Management rules

Management of Functional Safety
Requirements from IEC 61508 (4)

• All measures are to be planned and monitored
• Requirements necessary for the management of functional safety shall be formally reviewed and agreed
• All those identified as responsible for management of functional safety activities shall be informed of the responsibilities assigned to them
• Suppliers providing products or services to an organisation shall
  • deliver as specified by the organization
  • have an appropriate quality management system
Experience and qualification of all persons involved should be assessed and documented. Factors to be considered are:

- engineering knowledge appropriate to the application area
- safety engineering knowledge appropriate to the technology (e.g. electronic, software engineering)
- knowledge of the legal and safety regulatory framework

The required competence level depends on:

- the consequences in the event of failure of the E/E/PE safety-related systems
- the safety integrity level (SIL)
- the novelty of the design, design procedures or application

Competencies should be developed from previous experience:

- the greater the required competence levels, the closer the fit with the previous experience
KUGLER MAAG CIE is a service company with acknowledged expertise in process improvement

Facts
• Founded in 2004, today more than 75 acknowledged experts (average age 44)
• Specialized on process improvement
• Expertise in CMMI®, SPICE / ISO 15504, Functional Safety / IEC 61508, Project-, Quality-, Requirements-Mgmt., Change Management …

Industries
• Automotive Industry,
• Financial Services, ICT,
• Health, Telco and Railways

Customers
• Global players, culturally diverse, operating in
  • Europe,
  • North America and
  • Asia

Partners & Networks

KUGLER MAAG CIE Service Areas

Improvement Services
• Managing change for the purpose of lasting quality and productivity improvement
• Evaluating performance improvement potential

Process Application
• “Off-the-shelf” processes tailored for an accelerated and sustained process performance improvement
• Operational process execution

Change Engine Services
• Organizational change control
• Agile process management
• Strategy implementation

Appraisal Services
• Improvement “Readiness Check”
• Improvement “Health Check”
• CMMI® appraisals
• ISO/IEC 15504 / Automotive SPICE™ assessments

Knowledge Services
• Training and qualification of practitioners, EPG, quality group, assessors and (executive) management
• Training in relevant standards and their usage, including qualifying for customers’ or 3rd party assessments
• Public training as well as customized in-house training
KUGLER MAAG CIE Expert Areas

CMMI ®
- CMMI for Development
- CMMI for Acquisition
- CMMI for Services (Initial Draft)
- SEI Partner

SPICE
- Automotive SPICE™, ISO 15504
- Co-founder of iNTACS

Functional Safety
- IEC 61508
- ISO CD 26262

Project Management
- PMI, PMBoK
- Prince 2, OPM 3

Quality Management
- Quality Management, Assurance & Control
- TS 16949, ISO 9001, VDA 6.3, ...
- CMMI/PPQA, SPICE/SUP.1, ...

Requirements Engineering
- Management, analysis and elicitation of requirements

Mastering Change
- Ensure successful and sustainable organizational change

Performance-off-the-Shelf
- Accelerated and sustainable process performance improvement
- Project / Requirements / Quality Management Service Centre

We already work predominantly for international big companies in different industries, including:

- DBV-winterthur
- GE Money Bank
- AMB GENERALI
- DB Systel
- BEHR
- Continental
- Bosch
- Siemens VDO
- Siemens Transportation Systems
- Alcatel-Lucent
- Magneti Marelli
- Cobra Automotive Technologies
- Valeo
- TRW
- BMW Group
- Daimler
- Chrysler
- Delphi
- Olympus
- Sanden
- Equens
- Harman/Becker
- Automotive Systems
- Delphi
- Delphi
- Delphi
- Delphi
- Delphi
- Delphi
KUGLER MAAG CIE is a Key Player in the Automotive Industry, Acting in Different Roles

Customers
• OEMs like Daimler, Audi, BMW, Ford, GME, Porsche, Volkswagen and the majority of their suppliers of electronics and software

Standardization
• Supported the HIS in the definition and enhancement of assessment and process related standards
• Support of the VDA’s working group for software quality process and product standardization
• Active deployment of functional safety standards (IEC 61508, based on ISO CD 26262) together with customers
• Enhanced and extended the Automotive SPICE™ and Test Process Improvement approach for Automotive purposes

SPINs and Working Groups
• Initiator of conferences, SPINs, working groups and research activities like Lero Ireland & METI study, Japan

Typical Functional Safety Consultancy by KUGLER MAAG CIE

• On an organizational level
  • Definition and implementation of the company’s functional safety process
  • Optimization of company’s development processes, taking into account all requirements from IEC 61508, ISO CD 26262, CMMI and (Automotive) SPICE
  • Support in establishing a culture for functional safety
  • Performing trainings for the management of functional safety
    • Functional safety of software determined systems
    • Functional safety from the manager’s point of view

• On a per project level
  • Analysis of the suitability of the development process in order to support and enforce the achievement of the safety goals efficiently
  • Planning and implementation of appropriate measures
  • Coaching and operative support in implementing the project’s safety lifecycle. E.g.
    • Functional and Technical Safety Concept
    • Safety analyses
    • Preparation of the functional safety assessment
• ...has specific experiences with safety related projects and systems within the automotive industry
• ...has implemented the functional safety processes for first tier automotive suppliers delivering safety related equipment up to SIL3 / ASIL D. This included definition, training, coaching and rollout support for development projects.
• ...employees act as Functional Safety Managers
• ...has performed gap analysis regarding the implementation of functional safety requirements according to IEC 61508 and ISO CD 26262.
• The safety related coaching and supporting activities cover hazard and risk analysis, hardware and software architecture design and analysis (e.g. by FMEDA) and safety management with focus on the software safety lifecycle. The projects supported apply the IEC 61508 and/or the ISO CD 26262.

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

Peter Löw:
Mobile: +49 (0) 173-678 7347 Email: Peter.Loew@kuglermaag.com

Roland Pabst:
Mobile: +49 (0) 173-678 7351 Email: Roland.Pabst@kuglermaag.com

Dr. Erwin Petry
Mobile: +49 (0) 173-678 7337 Email: Erwin.Petry@kuglermaag.com
If you want to contact us …

• in the USA
  KUGLER MAAG CIE North America Inc.
  Mike Staszel
  Mobile: +1 313 727 9920
  Email: mike.staszel@kuglermaag.com
  http://www.kuglermaagusa.com

• in APAC
  KUGLER MAAG CIE
  Clemens Saur
  Mobile: +65 9168 0756
  Email: clemens.saur@kuglermaag.com

• in CEE
  KUGLER MAAG CIE
  Christophe Debou
  Mobile: +48 513 144 297
  Email: christophe.debou@kuglermaag.com
  Email: cee@kuglermaag.com

• in Italy
  KUGLER MAAG CIE
  Fabio Bella
  Mobile: +39 345 7019271
  Email: fabio.bella@kuglermaag.com