Importance of Functional Safety

Role of Process Improvement in Functional Safety

Confirmation Measures

Tying Related Standards/Models

ISO 26262 Audit & ASPICE Assessment

ISO 26262 Audit & ASPICE Assessment Results

* (Functional) Safety must not be a product of
  + The accidental skills of the management, developers, etc.
* But should be instead :
  + Reproducible
  + Verifiable
  + Embedded
    - Designed safely from the beginning
    - Cannot be created retrospectively by testing
* Standards/Models
  + Provide structured approach to give certainty in outputs
  + Especially when subject is complex (i.e., software)



IEC 62061

Machinery

IEC 62279

Rail Software

IEC 61508

ISO 26262

Automotive

IEC 61800-5-2

Electrical drives



IEC 61513

Nuclear Sector

IEC 60601

Medical devices

EN 50128

Railway

application

IEC 61511

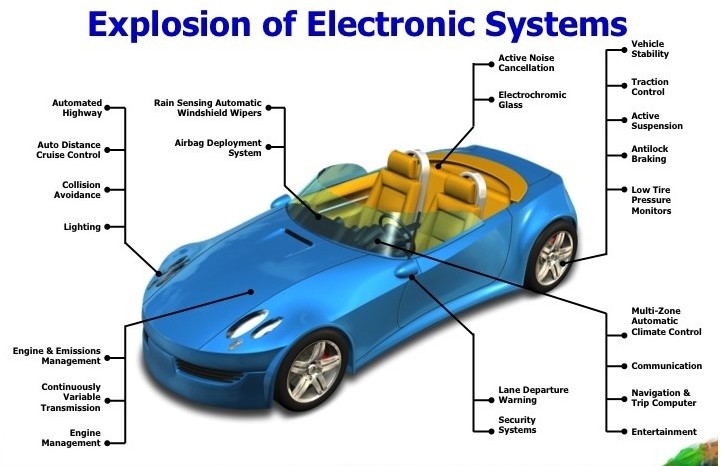
Process Sector

EN 50156

Furnaces

**Trend in Automotive Industry**

* Automotive industry increasingly driven by electrical, electronic or programmable electronic systems
* More than 80 percent of entire system is implemented in electronics and software
* Development becomes more and more challenging, requiring more formalized approach for performing activities
* Rapid increase in errors of ECUs
* Too many errors found during testing phase at OEM
* Complexity of ECUs in car continues to increase



Source: Chip Estimate blog

Importance of Functional Safety

Role of Process Improvement in Functional Safety

Confirmation Measures

Tying Related Standards/Models

ISO 26262 Audit & ASPICE Assessment

ISO 26262 Audit & ASPICE Assessment Results

# Reference : Automotive SPICE in ISO 26262

* ISO 26262 Part 2 - 2018

5 Overall safety management

5.3 Input to this clause

5.3.2 Further supporting information

- Existing evidence of compliance with standards that support quality management.

EXAMPLE 2: ISO/IEC 33000 series of standards, CMMI® or Automotive SPICE® series of standards regarding

product development

6 Project dependent safety management

6.4 Requirements and recommendations

6.4.11 Functional safety audit

Note 4: An organizations process definitions can address multiple standards at the same time, e.g., the ISO 26262 series of standards and Automotive SPICE® configuration management process requirements. This coordination of processes can help to avoid duplication of work or process inconsistencies. For these coordinated processes, organization-specific process cross-references to the requirements of the ISO 26262 series of standards and to Automotive SPICE® can be provided.

* Requirements to implement ISO 26262
  + Quality Management System
  + Organization wide Process Infrastructure
    - Standard safety process, procedure/guideline, templates, checklists, tools etc.
  + Continuous Process Improvement
  + All Engineering processes including system, software,
* The above are required at Automotive SPICE Capability level 3
* Ideally, achievement of Automotive SPICE Capability Level 3 is required for implementing ISO 26262.
  + However, this does not stop to initiate ISO 26262 implementation
* Organization wide processes can be defined by considering ISO 26262, Automotive SPICE and any other standards/models

**S**oftware **P**rocess **I**mprovement and **C**apability d**E**termination

* + Automotive SPICE is subset of SPICE
  + Basically, Automotive SPICE developed for software development projects
  + But Now ASPICE is extended to System development
  + Focus of Automotive SPICE and OEM is to determine Capability Levels
  + But Now Organization maturity is also possible by using intacs scheme or following ISO/IEC 330xx standards
  + Automotive SPICE is two-dimension model
    - Process Dimension defines processes
    - Process Capability defines the capability Levels

**CL 5**



**PA 5.2**

**PA 5.1**

**PA 4.2**

**PA 4.1**

**PA 3.2**

**PA 3.1**

**PA 2.2**

**PA 2.1**

**GPs, GRs**

**GPs, GRs**

**GP**

**BPs, WPs and W PCs**

**PA 1.1**

**Measurement framework**

**(ISO/IEC 33020)**

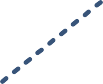
* **Capability levels**
* **Process attributes**
* Rating
  + Scale
  + Rating method
  + Aggregation method
* Process capability level model

|  |  |
| --- | --- |
| **Process assessment model**  **(Automotive SPICE)** |  |
| * **Process capability indicators** * **Process performance indicators** | |

**CL 4**

**CL 3**

**CL 2**

**CL 1**

**Outcomes of process 1**

**Outcomes of process 2**

**Outcomes of process 3**

**Process reference model (Automotive SPICE)**

* **Domain and scopes**
* **Process purposes**
* **Process outcomes**

ZooKoo Consulting Pvt. Ltd.

VDA Scope

2018, All rights reserved.

**Process Reference Model (PRM)**

**Process Outcomes:** 1) a strategy for perforing quality assurance is developed, implemented, and maintained;

2) quality assurance is performed independently and objectively without conflicts of interest;

**Purpose:** The purpose of the Quality Assurance Process is to provide independent and objective assurance that work products and processes comply with predefined provisions and plans and that non-conformances are resolved and further prevented.

**Base Practices:** SUP.1.BP1: Develop a project quality assurance strategy.

SUP.1.BP2: Assure quality of work products. SUP.1.BP3: Assure quality of process activities.

---

**Output work products:** 08-13 Quality Assurance -> [Outcome 1, 2]

13-04 Communication Record -> [Outcome 3, 4, 5]

---



**Work Products are specified**

Work products are produced according to specified procedures and are planned and tracked.

**2**



**Experience Factory**

Quantitative feedback is used to initiate improvement

activities; Measure impact of change and benefit.

**5**

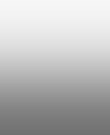


**Best Practices are selected**

Well defined process using tailored versions;

Organization widestandard process.

**3**



**Chaotic**

Output of phases not predictable

|  |  |
| --- | --- |
| ***Level 0: Incomplete process*** | |
| ***Level 1: Performed process*** | |
| ***PA 1.1*** | *Process performance process attribute* |
| ***Level 2: Managed process*** | |
| ***PA 2.1*** | *Performance management process attribute* |
| ***PA 2.2*** | *Work product management process attribute* |
| ***Level 3: Established process*** | |
| ***PA 3.1*** | *Process definition process attribute* |
| ***PA 3.2*** | *Process deployment process attribute* |
| ***Level 4: Predictable process*** | |
| ***PA 4.1*** | *Quantitative analysis process attribute* |
| ***PA 4.2*** | *Quantitative control process attribute* |
|  | |
| ***Level 5: Innovating process*** | |
| ***PA 5.1*** | *Process innovation process attribute* |
| ***PA 5.2*** | *Process innovation implementation process attribute* |

# Capability Dimension : PA 2.1 Performance Mgmt.

**Process Assessment Model (PAM)**

**ISO/IEC 33020**

**Result of Achievement :** a) Objectives for the performance of the process are identified;

b) Performance of the process is planned;

**Purpose:** The performance management process attribute is a measure of the extent to which the performance of the process is managed. As a result of full achievement of this process attribute:

**Generic Practices:** GP 2.1.1 Identify the objectives for the performance of the process. [ACHIEVEMENT a]

GP 2.1.2 Plan the performance of the process to fullfill identified objectives. [ACHIEVEMENT b]

---

**Generic Resources:** Human resources with identified objectives, responsibilities, authorities [ACHIEVEMENT e, f, h]

Facilities and infrastructure resources [ACHIEVEMENT g, h]

---

Importance of Functional Safety

Role of Process Improvement in Functional Safety

Confirmation Measures

Tying Related Standards/Models

ISO 26262 Audit & ASPICE Assessment

ISO 26262 Audit & ASPICE Assessment Results

* Confirmation review
  + Confirmation that a work product provides sufficient and convincing evidence of their contribution to the achievement of functional safety considering the corresponding objectives and requirements of ISO 26262
* Audit
  + Examination of an implemented process with regard to the process objectives
* Assessment
  + Examination of whether a characteristic of an item or element achieves the ISO 26262 objectives

# Confirmation Review

* The confirmation reviews are performed for those work products which are specified in ISO 26262 and required as per the safety plan
* A confirmation review includes the checking of correctness, completeness, consistency, adequacy and contents of the work products against corresponding requirements of ISO 26262
* A confirmation review and verification review may be combined, provided the review is performed with sufficient independence

# Functional Safety Audit

* Functional Safety Audit shall be carried out for items, whereof the highest ASIL among the safety goals is ASIL (B), ASIL C, ASIL D
* An evaluation of the implementation of the processes against the definitions of the activities referenced or specified in the safety plan
* The functional safety audit can be carried out by a qualified Automotive SPICE Assessor, then the functional safety audit and the Automotive SPICE assessment can be carried out simultaneously
* A functional safety assessment shall be carried out for items, whereof the highest ASIL among the safety goals is ASIL (B), C, or D
* The scope of a functional safety assessment shall include
  + the safety plan and all the work products required per the safety plan
  + the processes required for functional safety,
  + reviewing the appropriateness and effectiveness of the implemented safety measures that can be assessed during the item development.
* A functional safety assessment shall consider
  + the planning of the other confirmation measures
  + the results from the confirmation reviews and functional safety audit(s); and
  + the recommendation(s) resulting from the previous functional safety

assessment(s), if applicable

* A functional safety assessment report shall include a recommendation for acceptance, conditional acceptance, or rejection of the functional safety of the item.
  + Conditional acceptance shall only be given, if the functional safety of the item is achieved, subject to the resolution of the identified conditions of acceptances
  + In the case of conditional acceptance, the corrective actions provided in the functional safety assessment report should be carried out, and
  + In the case of rejection, adequate corrective actions shall be initiated and the functional safety assessment shall be repeated



# Level of independence

* Confirmation measures will be reviewed/audited/assessed by individuals who have sufficient level of knowledge
* Different level of independence to participant in different confirmation measures are considered in ISO 26262
  + I0 – the confirmation measures should be performed; and it shall be performed by a person other than author
  + I1 – the confirmation measures shall be performed; and it shall be performed by a person other than author
  + I2 – the confirmation measures shall be performed; and it shall be performed by a person who is independent from the team, which belong to author
  + I3 – the confirmation measures shall be performed; and it shall be performed by a person who is independent, regarding management, resources and release authority, from the department of author

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | | | | |  |
|  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Importance of Functional Safety

Role of Process Improvement in Functional Safety

Confirmation Measures

Tying Related Standards/Models

ISO 26262 Audit & ASPICE Assessment

ISO 26262 Audit & ASPICE Assessment Results