

Joint Quality Management in the Supply Chain

Automotive SPICE®

Potential Analysis

**Process Reference and Assessment Model
based on Automotive SPICE® and Automotive SPICE® for Cybersecurity
including Guidelines**

Joint Quality Management in the Supply Chain

Automotive SPICE® Potential Analysis

**Process Reference and Assessment Model
based on Automotive SPICE® and Automotive SPICE® for Cybersecurity
including Guidelines**

2nd edition, October 2026

Online Download Document

Non-binding VDA standard recommendation

The Association of the Automotive Industry (VDA) recommends its members to apply the following standard for the implementation and maintenance of quality management systems.

Exclusion of liability

This VDA volume is a recommendation available for general use. Anyone applying it is responsible for ensuring that it is used correctly in each case.

This VDA volume considers state-of-the-art technology, current at the time of issue. Implementation of VDA recommendations relieves no one of responsibility for their own actions. In this respect everyone acts at their own risk.

The VDA and those involved in VDA recommendations shall bear no liability.

If during the use of VDA recommendations, errors or the possibility of misinterpretation are found, it is requested that these be notified to the VDA immediately so that any possible faults can be corrected.

Copyright

This publication is protected by copyright. Any use outside of the strict limits of copyright law is not permissible without the consent of VDA and subject to prosecution. This applies in particular to copying, translation, microfilming and storage or processing in electronic systems.

Translations

This publication will also be issued in other languages. The current status must be requested from VDA QMC.

Trademark

Automotive SPICE® is a registered trademark of the Verband der Automobilindustrie e. V. (VDA).

For further information about Automotive SPICE® visit

www.vda-qmc.de.

Table of Content

Contents

Table of Content	III
Terms and glossary	6
1 Introduction	7
1.1 Scope	7
1.2 Statement of Compliance	8
1.3 Policies and Assumptions	8
1.3.1 Generic Rationales	8
1.3.2 Process specific Rationales	9
2 Process capability determination	10
2.1 Process reference model	10
2.1.1 Process specific rationales	12
2.2 Measurement framework	16
2.2.1 Process capability levels and process attributes	16
2.2.2 Process attribute rating	18
2.2.3 Rating and aggregation method	19
2.3 Process assessment model	19
2.3.1 Assessment indicators	19
2.4 Understanding the level of abstraction of a PAM	22
2.5 Why a PRM and PAM are not a lifecycle model and no blueprint for documentation	23
3 Process reference model and performance indicators	24
3.1 POPM Potential Project Management	24
3.2 RTCM Release and Technical Configuration Management	26
3.3 PQAS Process Quality Assurance	28
3.4 TEPR Technical Problem Resolution	30
3.5 SWDI Software Requirements, Design and Implementation	32
3.6 SWIV Software Integration and Verification	34
3.7 REEL Requirements Elicitation	36
3.8 SYRD System Requirements and Design	38
3.9 SYIV System Integration and Verification	40
3.10 MLEG Machine Learning Engineering	42
3.11 MLDM Machine Learning Data Management	44
3.12 PCOM Partner and Collaboration Management	46
3.13 TCRM Technical Change Request Management	48
3.14 CSGE Cybersecurity Goal Elicitation	50
3.15 CSVV Cybersecurity Verification and Validation	52
4 Consistency and traceability	54
4.1 Consistency and traceability within System Level and Software Level plugins	54
4.2 Relationships and traceability of Cybersecurity	55
5 Guideline	56
5.1 POPM Potential Project Management	56

5.1.1	General Information	56
5.1.2	Rating rules within the process	57
5.2	RTCM Release and Technical Configuration Management	58
5.2.1	General Information	58
5.2.2	Rating rules within the process	58
5.3	PQAS Process Quality Assurance	59
5.3.1	General Information	59
5.3.2	Rating rules within the process	59
5.4	TEPR Technical Problem Resolution Management	61
5.4.1	General Information	61
5.5	SWDI Software Requirements, Design and Implementation	62
5.5.1	General Information	62
5.5.2	Rating Rules within the process	62
5.6	SWIV Software Integration and Verification	64
5.6.1	General Information	64
5.6.2	Rating Rules within the process	64
5.7	REEL Requirements Elicitation	65
5.7.1	General Information	65
5.8	SYRD System Requirements and Design	66
5.8.1	General Information	66
5.8.2	Rating Rules within the process	67
5.9	SYIV System Integration and Verification	68
5.9.1	General Information	68
5.9.2	Rating Rules within the process	68
5.10	MLEG Machine Learning Engineering	69
5.10.1	General Information	69
5.10.2	Rating Rules within the process	69
5.11	MLDM Machine Learning Data Management	70
5.11.1	General Information	70
5.11.2	Rating Rules within the process	71
5.12	PCOM Partner and Collaboration Management	72
5.12.1	General Information	72
5.12.2	Rating Rules within the process	72
5.13	TCRM Technical Change Request Management	74
5.13.1	General Information	74
5.13.2	Rating Rules within the process	74
5.14	CSGE Cybersecurity Goal Elicitation	75
5.14.1	General Information	75
5.15	CSVV Cybersecurity Verification and Validation	76
5.15.1	General Information	76
Annex A	Conformity of the process assessment and reference model	77
Annex B	Information items characteristics	80
Annex C	Bibliography	93

Terms and glossary

Automotive SPICE® Potential Analysis consists of a subset of Automotive SPICE® 4.1 and Automotive SPICE® for Cybersecurity 2.0. Terms and definitions are not repeated here and can be referred to in the respective volumes.

Please refer to [ISO33001] for a full glossary of the terms used in the ISO/IEC 330xx series.

1 Introduction

1.1 Scope

The Automotive SPICE® Potential Analysis (ASPICE PoA) provides a standardized method to support the evaluation of the capability of a potential collaboration or partnership to realize and deliver a planned product or service. This is not limited to customer-supplier relations only.

The Automotive SPICE® Potential Analysis is intended to be used as a precondition to a customer awarding a contract for a specific product or service or to substitute a missing (Automotive SPICE®) Supplier Self Evaluation (SuSE).

For nominated or established partners, the application of Automotive SPICE® Potential Analysis can reduce risk by evaluating whether a partner is able to realize products within the established organization in the context of constraints or other limitations from the customer. Additionally, Automotive SPICE® Potential Analysis can be used for process improvement, e.g., to support problem analysis efforts.

The Automotive SPICE® Potential Analysis is applicable to all types of software-based systems including Commercial of the shelf (COTS) and legacy content if suitable and appropriate.

Since an evaluation of partners with the Automotive SPICE® Potential Analysis is only based on an exemplary project, the result is only valid to a very limited extent. Use of the conclusions over a longer period, or changed conditions, should be avoided.

Results of Automotive SPICE® Potential Analyses are only representative for a limited period. The duration of the acceptance period must be agreed between the partners.

Compared to an Automotive SPICE® 4.x Assessment, the Automotive SPICE® Potential Analysis has a reduced content. It focuses on capability level 1 and requires a smaller number of samples to be evaluated and therefore less time, the availability of which is often very limited in a nomination phase or in critical project situations.

An Automotive SPICE® Potential Analysis can be used as a first step to reach a defined Automotive SPICE® level. It may follow a supplier self-evaluation or directly represent the first step towards an agreed capability level. In any case, identified weaknesses can serve as input to an improvement program to prepare for a full Automotive SPICE® 4.x Assessment without another prior Potential Analysis. As such, the Automotive SPICE® 4.x Assessment also intends to increase the acceptance and application of Automotive SPICE®.

Automotive SPICE® Potential Analysis is based on the contents of Automotive SPICE® 4.1 and Automotive SPICE® for Cybersecurity 2.0, contains only a subset of these volumes and is not an extension to them. Evaluation has to be done in relation to this reduced content, therefore the assessors' understanding of completeness has to be aligned to it. The individual reasons and motivation of the reduction are described as "Rationales".

The evaluation considers the changed purpose of the Automotive SPICE® Potential Analysis. A different assessment rating scheme is also used to differentiate its results to Automotive SPICE® 4.x Assessment results.

The Automotive SPICE® Potential Analysis follows the same principles of Automotive SPICE® with methodological freedom and individually assessable processes.

This current version was extended to cover also Machine Learning based on the [ISO/PAS8800].



Figure 1 — Purpose of Automotive SPICE® 4.0 Assessment vs. Automotive SPICE® Potential Analysis

The purpose of the Automotive SPICE® Potential Analysis is comparable to the potential analysis in VDA QMC Volume 6 Part 3 (1), which is a subset of the standard questions. The VDA 6.3 potential analysis (module P1 of the questionnaire) is an established method for carrying out a risk assessment. It is used to quantify the risk for suppliers, new technologies, new locations, or new products.

While the VDA 6.3 potential analysis is an extract from the VDA 6.3 requirements catalog, the Automotive SPICE® Potential Analysis is exclusively focused on the development of software systems as an independent PAM/PRM, not including any hardware or mechanical aspects.

1.2 Statement of Compliance

The Automotive SPICE® Potential Analysis, and its process reference model conform with the requirements of ISO/IEC 33004:2015 and can be used as the basis for conducting an assessment of process performance capability under consideration of policies and assumptions. The Automotive SPICE® Potential Analysis Process measurement framework fulfills conformance to the requirements of ISO/IEC 33003:2015.

1.3 Policies and Assumptions

(4.1.1) g) The measurement framework shall document the policies and assumptions underlying its use and application; (ISO/IEC 33003:2015)

The Automotive SPICE® Potential Analysis is based on Automotive SPICE® 4.0 and Automotive SPICE® for Cybersecurity, with specific deviations. These deviations can be of following 2 types:

- **Rationales of generic character (RAG.X) reflecting specific circumstances for all processes.**
- **Rationales of process specific character (RAP.X), which affect one or a few processes only.**

Rationales provide justification for differences between Automotive SPICE® Potential Analysis and the combination of Automotive SPICE® 4.0 and Automotive SPICE® for Cybersecurity. They outline reasons for those limitations to improve the understanding of the PAM/PRM in general. For example, Rationales may outline systematic and logical dependencies as well as deviations that are motivated for only efficiency increase of the assessment process itself.

1.3.1 Generic Rationales

Rationale RAG.1 "**Resources**" of human capital and personnel in a project are not in the scope of the ASPICE PoA because the premise of the inspected projects will likely differ from those for the final customer. The evaluation of the estimation approach therefore concentrates on effort estimation, suitability and appropriateness rather than accuracy and prudence in resources allocation.

Rationale RAG.2 “**Scope of work**” documentation is not inspected in ASPICE PoA as the completeness of the full project work and its boundaries is not relevant for the purpose of the ASPICE PoA. Consequently, the main objective project reference is the project schedule.

Rationale RAG.3 “**Feasibility**” evaluation in ASPICE PoA is limited to the technical feasibility inspection of the project and the monitoring of the project schedule. The consistency between effort estimation and resource availability cannot be evaluated due to *RAG.1 “Resources”*. Furthermore, the qualification of resources is also not evaluated in ASPICE PoA (see also *RAG.4 “Responsibilities”*).

Rationale RAG.4 “**Responsibilities**” of roles and individuals in ASPICE PoA are only exemplary. Their availability and role fulfillment may change in following and other projects for a changed scope and qualification profile. Consequently, the qualification of roles is not evaluated systematically within the ASPICE PoA.

Rationale RAG.5 “**Communicate and agree**” Due to *RAG.1 “Resources”* and *RAG.4 “Responsibilities”*, effective communication between the project stakeholders itself is not an objective of the ASPICE PoA. Instead, the outcomes of stakeholder activities are to be evaluated independently of communication. As a consequence, there cannot be a complete or consistent evaluation of agreements of stakeholders on such communication. In addition to these circumstances, reports as outcomes from processes are consequently removed from ASPICE PoA for efficiency reasons.

1.3.2 Process specific Rationales

Policies and assumptions result from context, purpose, and generic rationales for individual, process specific deviations. Those are consequently limited in general and consider also typical effort, elimination of redundancy and effectiveness for valid rationales for single or a small number of related processes. The process specific rationales are to be found in detail after the reference model to improve the readability of the document. They are listed within chapter 2.1.1.

2 Process capability determination

2.1 Process reference model

Processes defined in the Automotive SPICE® Potential Analysis model are independent from each other and there is no process group definition. It mandates the review of the BASIC scope, consisting all of its 4 BASIC scope processes, and at least one plugin. The BASIC scope forms the core element, the minimum scope of the Automotive SPICE® Potential Analysis.



Figure 2 — Processes of the BASIC scope

The four Automotive SPICE® Potential Analysis plugins allow a suitable scope selection for either System Level, Software Level, Requirements Elicitation, or Machine Learning.

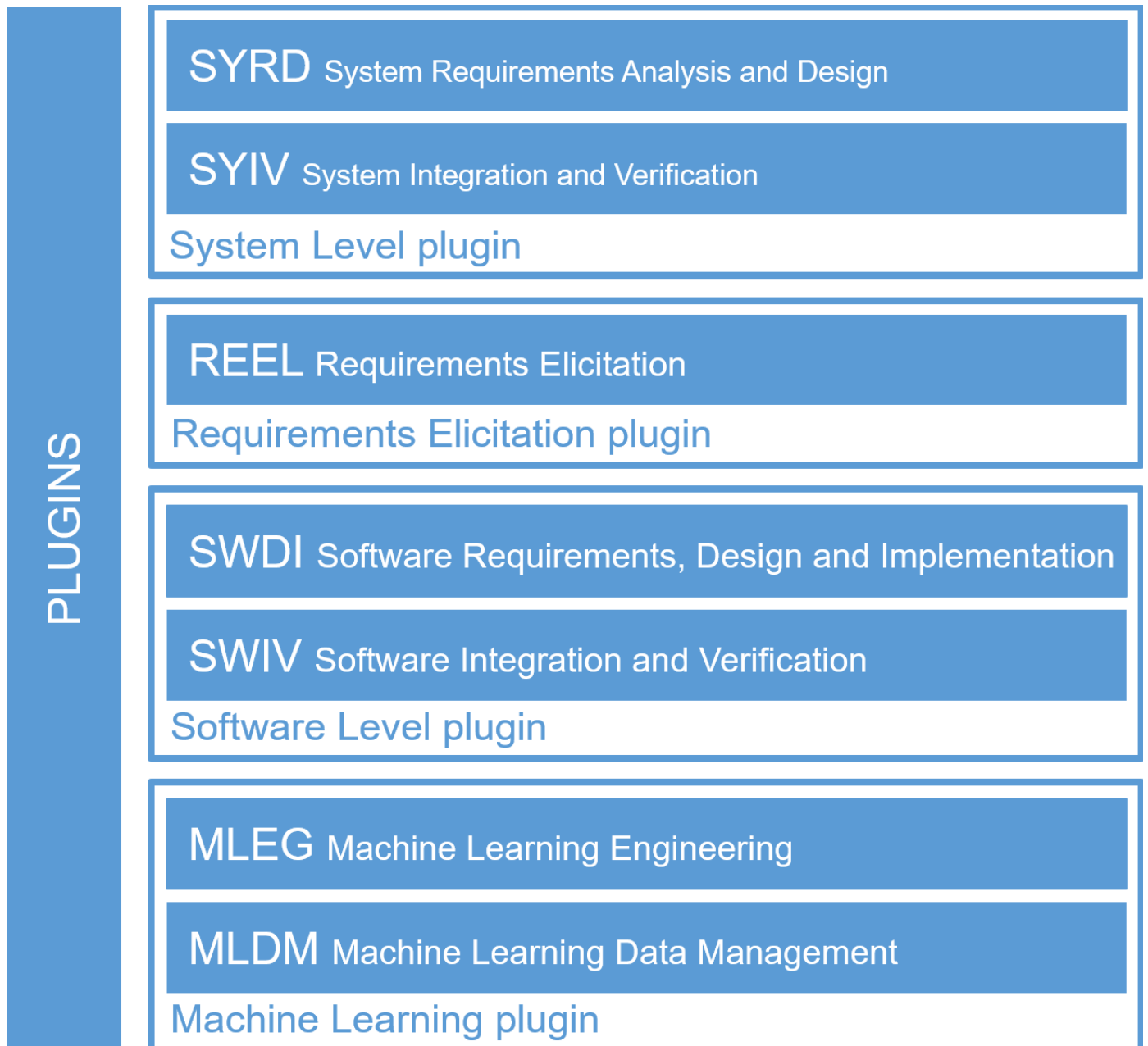


Figure 3 — The four plugins and their processes in the Automotive SPICE® Potential Analysis

Optional processes can be selected individually within the FLEX scope of the Automotive SPICE® Potential Analysis.



Figure 4 — Optional Processes for FLEX scope

2.1.1 Process specific rationales

Rationale RAP.1 “**Process assurance only**”: The ASPICE PoA puts a focus on the technical evaluation and does not consider most organizational supporting aspects. Therefore, work products and other information items may not be sufficiently reviewable within its scope. The Process Quality Assurance (PQAS) process therefore is reduced to the verification of process assurance. The ASPICE PoA refers to this aspect within Process Quality Assurance (PQAS).

Rationale RAP.2 “**Organizational aspects**” in the ASPICE PoA are very limited for the prioritization of technical, engineering aspects and Capability Level 1 as the highest achievable level. The ASPICE PoA aims to reduce the evaluation of interfaces that are not directly related to technical efforts also for efficiency reasons. Thus, one may exclude interfaces to stakeholders such as marketing, human resources management, competency management and others that often are in shared groups within organizations. The ASPICE PoA refers to organizational aspects for related problems in Potential Project Management (POPM), but only technical problems within Technical Problem Management (TEPR) and technical related change requests within the Technical Change Request Management (TCRM).

Rationale RAP.3 “**Risk identification**” is not included within the Potential Project Management (POPM) process for efficiency reasons, as a consequence of *RAG.1 “Resources”* and *RAP.2 “Organizational aspects”*. The number of sources, interfaces and stakeholders may be different in other project configurations. Therefore, only the capability to manage already identified and available risks is in the focus of the Potential Project Management (POPM) process. Completeness of these inputs is consequently also out of scope. The ASPICE PoA refers to this aspect in Potential Project Management (POPM).

Rationale RAP.4 “**Identification of problems**” is not evaluated within the ASPICE PoA, analogous to the Rationale *RAP.3 “Risk identification”*. The evaluation of capabilities to document and manage available technical problems is of higher interest than the identification process. The ASPICE PoA refers to this aspect within Technical Problem Resolution (TEPR).

Rationale RAP.5 “**Urgent resolution and alert**” are omitted in ASPICE PoA due to efficiency reasons. The identification and handling of such technical problems can be very time consuming and may also require inspection of separate organization structures. With the restricted scope of the ASPICE PoA this cannot be consistently evaluated. The ASPICE PoA refers to this aspect within Technical Problem Resolution (TEPR).

- Rationale RAP.6 “**Tracking problems to change requests**” is not evaluated in the ASPICE PoA due to the difficulty to identify and observe sufficient evidence to demonstrate the relationships and scenarios in the context of an ASPICE PoA.
The ASPICE PoA refers to this aspect within Technical Problem Resolution (TEPR).
- Rationale RAP.7 “**Technical changes only**”: There can be two different kinds of change requests: technical changes and organizational changes. Technical changes address the intended product directly. They typically influence the requirement set and originate in changed or specified stakeholder needs. Like Technical Problem Resolution (TEPR), Technical Change Request Management (TCRM) focusses on technically relevant items for efficiency reasons and as a consequence of *RAG.1 “Resources”* and *RAG.4 “Responsibilities”*.
The ASPICE PoA refers to this aspect within Technical Change Request Management (TCRM).
- Rationale RAP.8 “**Review of implementation**” and “**Approval before implementation**” of a change request is omitted within Technical Change Request Management (TCRM) for efficiency reasons. Tracking to closure is part of the ASPICE PoA which evaluates how well the change is actually implemented and checked respectively.
The aspect of an in-depth change request analysis as basis for the approval is of a higher priority than the approval itself in the ASPICE PoA.
The ASPICE PoA refers to this aspect within Technical Change Request Management (TCRM).
- Rationale RAP.9 “**Configuration items**”: Engineering related configuration items shall be evaluated in Release and Technical Configuration Management (RTCM) for processes in the chosen scope only (see Figure 3 and Figure 4). Other non-technical related configuration items are not considered in the Release and Technical Configuration Management (RTCM) process because the scope reduction of the ASPICE PoA renders them insufficiently assessable within the exemplary project.
The ASPICE PoA refers to this aspect within Release and Technical Configuration Management (RTCM).
- Rationale RAP.10 “**Baseline completeness and consistency**”: In the Release and Technical Configuration Management (RTCM) process only the technical and engineering specific configuration items are considered. See also Rationale *RAP.2 “Organizational Aspects”*. Consequently, the completeness and consistency of the baselines cannot be verified in the ASPICE PoA as other configuration items may be required for a complete evaluation.
The ASPICE PoA refers to this aspect within Release and Technical Configuration Management (RTCM).
- Rationale RAP.11 “**Delivery**”: The ASPICE PoA Release and Technical Configuration Management (RTCM) does not differentiate between internal or external deliveries, as both types of deliveries require the same level of detail in the case of distributed and interconnected development.
The ASPICE PoA refers to this aspect within Release and Technical Configuration Management (RTCM) and Partner and Collaboration Management (PCOM).
- Rationale RAP.12 “**Access rights**” control is nowadays highly dependent on IT infrastructure, policies, personal data regulation (e.g., GDPR in European legislation). The Release and Technical Configuration Management (RTCM) in ASPICE PoA does not consider this topic due to the large amount of project independent indicators and sensitive data needed to be reviewed.
The ASPICE PoA refers to this aspect within Release and Technical Configuration Management (RTCM).
- Rationale RAP.13 “**Partner and Collaborations**”: The ASPICE PoA reflects these terms as they are used in publications to describe more complex collaboration scenarios, in which the traditional customer-supplier relationship is only one of the many scenarios. Partnership and collaborations may include the role of providing and receiving services at different phases in accordance with any type or form of written agreements.
The ASPICE PoA refers to this aspect within Partner and Collaboration Management (PCOM).

- Rationale RAP.14 **“Quotation and contracts”**: In ASPICE PoA contracts and commercial agreements for quotation must not be considered. The information in such documents may lead to a risk of compliance violations and other legal problems for assessors, participants, and the assessment team. The evaluation should instead refer to the quotation and selection process to reach an agreement with a potential partner and for a potential collaboration.
The ASPICE PoA refers to this aspect within Partner and Collaboration Management (PCOM).
- Rationale RAP.15 **“Scope of cybersecurity”**: Analogous to *RAG.2 “Scope of work”*, the activities of cybersecurity management are only exemplary. The scope including the assets, cybersecurity properties, stakeholders, product phases and impact categories may be different in other project configurations. Therefore, the boundaries and completeness of such a scope definition are not to be evaluated and such an evaluation is not an objective of the ASPICE PoA.
The ASPICE PoA refers to this aspect within Cybersecurity Goal Elicitation (CSGE) and Cybersecurity Verification and Validation (CSVV).
- Rationale RAP.16 **“Prioritization of threats”** before their evaluation is not relevant for the Cybersecurity Goal Elicitation (CSGE) process as a consequence of *RAP.15 “Scope of cybersecurity”*. A consistent evaluation would not be possible due to the missing context in this case.
The ASPICE PoA refers to this aspect within Cybersecurity Goal Elicitation (CSGE).
- Rationale RAP.17 **“Monitoring risks of cybersecurity”**: A systematic review of cybersecurity related monitoring and control is beyond the scope of the Automotive SPICE® Potential Analysis. It would require inspection of project and organizational interfaces for current and historic evaluations on a selection of trigger and event criteria. A partial inspection would be inappropriate and result in a high risk of vague and incomplete indicators for a rating. Therefore, ASPICE PoA does not inspect the reiteration and control cycle for related changes impacting cybersecurity during the conduct of an exemplary project.
The ASPICE PoA refers to this aspect within Cybersecurity Goal Elicitation (CSGE) and Cybersecurity Verification and Validation (CSVV).
- Rationale RAP.18 **“Vulnerability Analysis”** requires an interaction and transparency at project and organizational level. This would include prerequisites to Cybersecurity Management practices, for example as stated in ISO/SAE 21434. Since the possibility to inspect these within an ASPICE PoA is not always given, vulnerability analysis is not considered.
The ASPICE PoA refers to this aspect within Cybersecurity Verification and Validation (CSVV).
- Rationale RAP.19 **“Cybersecurity Risk Treatment Implementation”** is not evaluated within the ASPICE PoA for efficiency reasons. The ASPICE PoA aims on a high-level evaluation of cybersecurity and refers to this aspect within Cybersecurity Verification and Validation (CSVV).
- Rationale RAP.20 **“Obtain stakeholder expectations and requests”**: Focus of the ASPICE PoA is on technical stakeholders and their direct input, see *RAP.2 “Organizational aspects”*, *RAP.4 “Identification of problems”* and *RAP.7 “Technical changes only”*.
Despite the fact that requirement elicitation typically focuses on customer needs, stakeholders encompass more than just the customers, as they include all other relevant sources of needs and requirements such as legal, regulatory, industrial standards as well as internal organizations. Within the flexible plugin model of the ASPICE PoA (i.e. Requirements Elicitation, System Level and Software Level plugins), "stakeholder" can be generally interpreted as input-relevant sources of needs and requirements for the corresponding level of engineering to be evaluated. E.g., the system discipline could also be a possible stakeholder for software engineering. The ASPICE PoA refers to this aspect within Requirements Elicitation (REEL).
- Rationale RAP.21 **“Prioritization of requirements”**: is limited to the scope of the project schedule within the ASPICE PoA.
The ASPICE PoA refers to this aspect within Software Requirements, Design and Implementation (SWDI) and System Requirements Analysis and Design (SYRD).

Rationale RAP.22 “**Select verification measures**”: The selection of individual verification measures is a practice to be reviewed in more complex test setups, e.g., to control verification according to various configurations as well as target variants. The ASPICE PoA does not foresee to review complex variant configurations, but focuses instead on a specific release configuration. The ASPICE PoA refers to this aspect within Software Integration and Verification (SWIV) and System Integration and Verification (SYIV).

Rationale RAP.23 “**Cross relationships**” between following named processes shall not be considered for simplification reasons: Potential Project Management (POPM), Release and Technical Configuration Management (RTCM), Process Quality Assurance (PQAS), Technical Problem Resolution (TEPR), Technical Change Request Management (TCRM) and Partner and Collaboration Management (PCOM). This avoids or at least reduces the need to return to already assessed processes within the assessment and in general also improves the separation of processes and assessment indicators. Assessors must only choose and evaluate evidence for indicators such that their origin and end point are both affecting the same process. The ASPICE PoA refers to this aspect within Potential Project Management (POPM), Release and Technical Configuration Management (RTCM), Process Quality Assurance (PQAS), Technical Problem Resolution (TEPR), Technical Change Request Management (TCRM), and Partner and Collaboration Management (PCOM).

Rationale RAP.24 “**Impact on ML operating environment**” is not evaluated explicitly within the ASPICE PoA for efficiency reasons, due to the large variance of suitable target environments. The ASPICE PoA refers to this aspect within Machine Learning Engineering (MLEG).

Rationale RAP.25 “**ML Architecture**” is not evaluated explicitly within the Machine Learning Engineering (MLEG) in the ASPICE PoA for efficiency and simplification reasons. A successful validation indicates that a valid ML architecture is implemented.

Rationale RAP.26 “**ML data management**” (MLDM) is an essential aspect of machine learning engineering and is therefore considered within the PoA to an appropriate extent.

2.2 Measurement framework

The measurement framework provides the necessary requirements and rules for the capability dimension. It defines a scheme which enables an assessor to determine the Capability Level of a given process. These capability levels are defined as part of the measurement framework.

To enable the rating, the measurement framework provides process attributes defining a measurable property of process capability. Each process attribute is assigned to a specific capability level. The extent of achievement of a certain process attribute is represented by means of a rating based on the defined rating scale. The rules from which an assessor can derive the final capability level for a given process are represented by a process capability level model.

The Automotive SPICE® Potential Analysis defines its own measurement framework.

NOTE: ISO/IEC 33020:2019 process attribute definitions and attribute outcomes are duplicated from ISO/IEC 33020:2019 in italic font and marked with a left side bar.

2.2.1 Process capability levels and process attributes

The definition of process capability indicators for each process attribute is an integral part of the measurement framework. Process capability indicators such as generic practices and information items are the means to support the judgement of the degree of achievement of the associated process attribute.

This chapter defines the generic practices and information items and their mapping to the process attributes for each capability level of the Automotive SPICE® for Potential Analysis' measurement framework.

Process capability level	Process attribute ID Process attribute name Process attribute scope Process attribute achievements	Each process attribute is identified with a unique identifier and name. A process attribute scope statement is provided, and process achievements are defined.
Process attribute achievement indicators	Generic practices	A set of generic practices for the process attribute providing a definition of the activities to be performed to accomplish the process attribute scope and fulfill the process attribute achievements. The generic practice headers are summarized at the end of a process to demonstrate their relationship to the process attribute achievements.
	Output information items	The output information items that are relevant to accomplish the process attribute scope and fulfill the process attribute achievements are summarized at the end of a process attribute section to demonstrate their relationship to the process attribute achievements. <i>Note: Refer to Annex B for the characteristics of each information item.</i>

2.2.1.1 Process capability Level 0: Incomplete process

The process is not implemented, or fails to achieve its process purpose. At this level there is little or no evidence of any systematic achievement of the process purpose.

Due to lack of a defined process attribute for process capability level 0, no generic practices and information items are defined for it.

2.2.1.2 Process capability Level 1: Performed process

For the Automotive SPICE® Potential Analysis' highest capability level (Level 1: Performed process) there is one process attribute defined: *Process Performance*.

2.2.1.3 PA 1.1 Process performance process attribute

Process attribute ID
PA 1.1
Process attribute name
Process performance
Process attribute scope
<i>The process performance process attribute is a measure of the extent to which the process purpose is achieved.</i>
Process attribute achievements
<i>As a result of full achievement of this process attribute: The process achieves its defined outcomes.</i>

Generic practices
GP 1.1.1 Achieve the process outcomes
Achieve the intent of the base practices.
Produce work products that evidence the process outcomes.

PA 1.1 Process performance process attribute	Achievement a
Output Information Items	
Process specific information items, as described in chapter 3	X
Generic practices	
GP 1.1.1 Achieve the process outcomes	X

The process capability level to be achieved for Level 1 by a process shall be derived from the process attribute rating for that process according to the process capability level model defined in Table 1.

2.2.2 Process attribute rating

To support the rating of process attributes, the measurement framework rating scale for the Automotive SPICE® Potential Analysis is defined in this chapter. For Automotive SPICE® Potential Analysis, the rating is restricted to Class 3 assessments only (see Annex A).

Process capability level 0 does not include any type of indicators, as it reflects a non-implemented process or a process which achieves only fragmentary process performance.

Scale	Process attribute	Rating color	Rating
Level 1	PA 1.1: Process Performance	Yellow	Valid

Table 1 — Level 1 Process performance process attribute minimum rating definition

2.2.2.1 Rating scale

Within this process measurement framework, a process attribute is a measurable property of process capability. A process attribute rating is a judgement of the degree of achievement of the process attribute for the assessed process.

The rating scale of Automotive SPICE® Potential Analysis is shown in Table 2.

Characteristic judgement for degree of achievement	Rating color	Rating
There is little or no evidence of achievement of the process performance process attribute in the assessed process.	Red	Fragmentary
There is evidence of a significant achievement of the process performance process attribute. Some weaknesses may exist, but they do not interfere with a valid systematic approach in the assessed process. <i>Note: This includes documented and highlighted weaknesses that may become challenges for later phases of an intended collaboration and may require early improvement actions.</i>	Yellow	Valid
There is evidence of a satisfactory achievement of the process performance process attribute. There are no or only minor weaknesses without impact of achieving the purpose of the assessed process.	Green	Satisfactory

Table 2 — Rating scale and characteristics of the Automotive SPICE® Potential Analysis.

The ordinal scale defined above shall be understood in terms of percentage achievement of a process attribute.

Percentage of achievement	Rating color	Rating
0 to ≤ 50% achievement	Red	Fragmentary
> 50% to ≤ 75% achievement	Yellow	Valid
> 75% to ≤ 100% achievement	Green	Satisfactory

Table 3 — Rating scale percentage values

2.2.3 Rating and aggregation method

Rating and aggregation method references are taken from [ISO33020], which provides the following definitions:

A process outcome is the observable result of successful achievement of the process purpose.

A process attribute outcome is the observable result of achievement of a specified process attribute.

Process outcomes and process attribute outcomes may be characterized as an intermediate step to providing a process attribute rating.

When performing rating, the rating method employed shall be specified relevant to the class of assessment. The following rating methods are defined.

The use of rating method may vary according to the class, scope and context of an assessment. The lead assessor shall decide which (if any) rating method to use. The selected rating method(s) shall be specified in the assessment input and referenced in the assessment report.

The rating method in the Automotive SPICE® Potential Analysis is *Rating method R3*.

[ISO33020] provides references to 3 rating methods, provides the following definition for Rating method R3:

....

Rating method R3

Process attribute rating across assessed process instances shall be made without aggregation.

2.3 Process assessment model

The process assessment model offers indicators to identify whether the process outcomes and the process attribute outcomes (achievements) are present or absent in the instantiated processes of projects. These indicators provide guidance for assessors in accumulating the necessary objective evidence to support judgments of capability. They are not intended to be regarded as a mandatory set of checklists to be followed.

2.3.1 Assessment indicators

According to [ISO33004], a process assessment model needs to define a set of assessment indicators:

Assessment Indicators

A process assessment model shall be based on a set of assessment indicators that:

- a) explicitly address the purpose and process outcomes, as defined in the selected process reference model, of each of the processes within the scope of the process assessment model;*
- b) demonstrate the achievement of the process attributes within the scope of the process assessment model;*
- c) demonstrate the achievement (where relevant) of the process quality levels within the scope of the process assessment model.*

The assessment indicators generally fall into three types:

- a) **practices** that support achievement of either the process purpose or the specific process attribute.*
- b) **information items** and their characteristics that demonstrate the respective achievements.*
- c) **resources and infrastructure** that support the respective achievements.*

In the Automotive SPICE® Potential Analysis assessment model, only **practices** and **information items** are used as assessment indicators.

Practices represent activity-oriented indicators, whereas information items represent result-oriented indicators. Both practices and information items are used for judging objective evidence to be collected and accumulated in the performance of an assessment.

As a first type of assessment indicator, practices are provided, which can be divided into two types:

1. Base practices (BP), applying to capability level 1

They provide an indication of the extent of achievement of the process outcomes. Base practices relate to one or more process outcomes, thus being always process-specific and not generic.

2. Generic practices (GP), applying to capability level 1

They provide an indication of the extent of process attribute achievement. Generic practices relate to one or more process attribute achievements, thus applying to any process.

As a second type of assessment indicators, **information items (II)** including their **characteristics (IIC)** are provided in Annex B. These are meant to offer a good practice and state-of-the-art knowledge guide for the assessor. Therefore, information items including their characteristics are designed to be a quickly accessible information source during an assessment.

Information item characteristics shall not be interpreted as a required structure of a corresponding work product, which is to be defined by the project and organization, respectively. Please refer to chapter 0 for understanding the difference between information items and work products.

[ISO33004] requires the mapping of assessment indicators to process attributes as shown in Figure 5.

The capability of a process on level 1 is only characterized by the measure of the extent to which the process outcomes are achieved. According to ISO 33003:2015, a measurement framework requires each level to incorporate at least one process attribute. The process attribute PA1.1 is defined for capability level 1 as the only process attribute at this level, and this process attribute has a single generic practice (GP1.1.1) pointing as an editorial reference to the respective process performance indicators (see Figure 5 and examples in Figure 6 and Table 4).

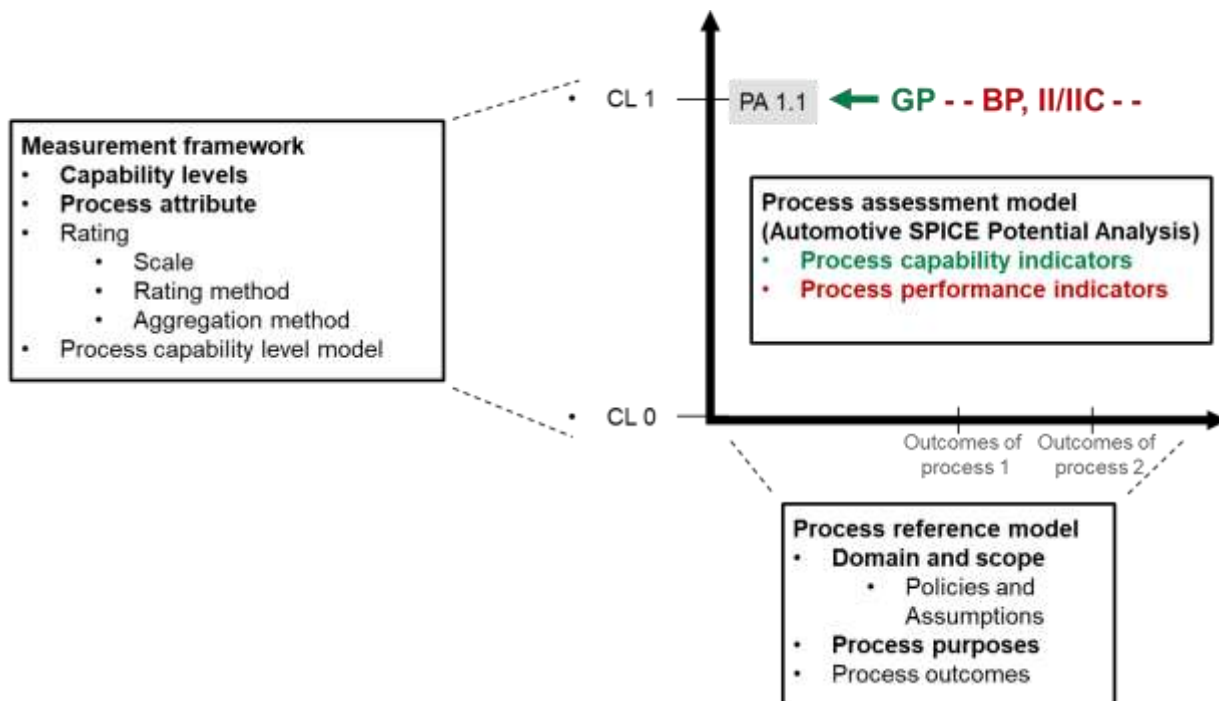


Figure 5 — Mapping model ASPICE PoA

Figure 6 and Table 4 show an exemplary result of an Automotive SPICE® Potential Analysis in form of a graph and a table.

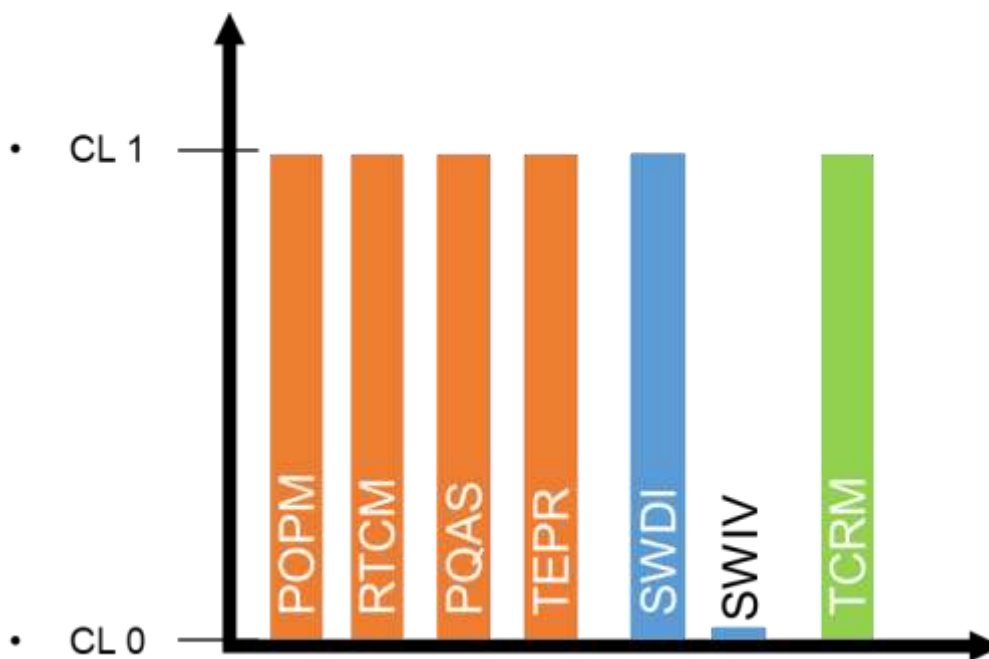


Figure 6 — Capability level per process (example)

Process ID	PA 1.1	CL1
POPM	Green	Yes
RTCM	Green	Yes
PQAS	Yellow	Yes
TEPR	Yellow	Yes
SWDI	Green	Yes
SWIV	Red	No
TCRM	Yellow	Yes

Table 4 — Process attribute rating and capability level achievement per process (example)

2.4 Understanding the level of abstraction of a PAM

The term “process” can be understood at three levels of abstraction. Note that for the term “process” there are different abstraction levels, and that a PAM resides at the highest.



Figure 7 — Possible levels of abstraction for the term “process”

Capturing experience acquired during product development (the DOING level) in order to share this experience with others means creating a HOW level. The HOW is specific to the context of an exemplary project for the Automotive SPICE® Potential Analysis PAM.

2.5 Why a PRM and PAM are not a lifecycle model and no blueprint for documentation

A lifecycle model defines phases and activities in a chronological order, possibly including cycles or loops, and parallelization. For example, some standards such as ISO 26262 or ISO/SAE 21434 are centered around a lifecycle model (neither of these standards in fact represents a PRM according to [ISO33004]). Companies, organizational units, or projects will interpret such general lifecycle models given in standards, and then derive roles, organizational interactions and interfaces, tools or tool chains, work instructions, and artifacts. Lifecycle models therefore are a concept at the HOW level (see chapter 2.4).

In contrast, a PRM/PAM according to [ISO33004] (formerly ISO/IEC 15504-2) is at the level of the WHAT by abstracting from any HOW level, see Figure 7 in chapter 2.4. A PRM/PAM groups a set of coherent and related characteristics of a particular technical topic and calls it 'process'. In different terms, a process in a PRM represents a 'distinct conceptual silo'. In this respect, a PRM/PAM

- neither predefines, nor discourages, any order in which PRM processes or Base Practices are to be performed.
- does not predefine any particular work product structure, or work product blueprints. Within ASPICE Potential Analysis there is no formal work product definition, whereas technical standards like [ISO21434] or [ISO26262] include such and provide detailed requirements for them.

As a consequence, it is the assessor's responsibility to perform a mapping of elements in such a HOW level to the Assessment Indicators in the PAM, see Figure 8.

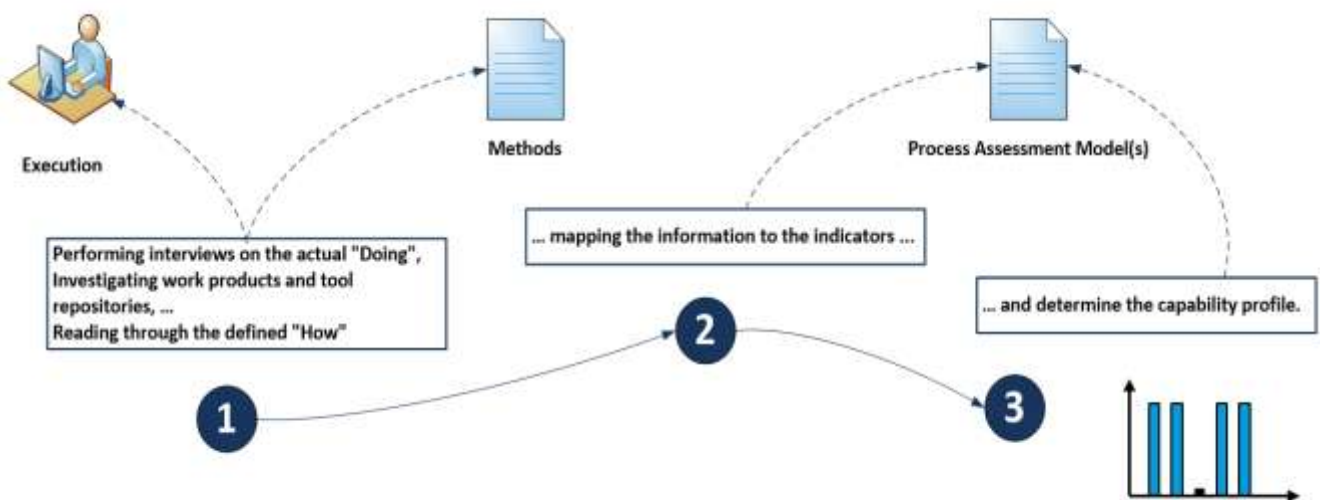


Figure 8 — Performing a process assessment for determining process capability profile

3 Process reference model and performance indicators

3.1 POPM Potential Project Management

Process ID
POPM
Process name
Potential Project Management
Process purpose
The purpose is to identify and manage the activities of an exemplary project to develop a product, manage the risks and monitor the organizational problems related to the project.
Process outcomes
1) The activities are identified, sized, and estimated. 2) Technical feasibility of the activities is evaluated. 3) The interfaces of the project are identified and monitored. 4) Schedule for execution of the project is developed and monitored. 5) Progress of the activities is reviewed. 6) The risks are managed continuously. 7) The organizational problems related to the project are recorded, analyzed, and monitored.

Base Practices
POPM.BP1: Identify, define, and estimate the activities. Define the estimates of effort for the identified project activities and document the dependencies. POPM.BP2: Ensure technical feasibility. Evaluate technical feasibility of activities and goals within the project's constraints on time and estimates. POPM.BP3: Identify and monitor the project interfaces. Identify and monitor the interfaces of the project with internal or external stakeholders. <i>Note 1: Interfaces for partnerships and collaborations based on goods and work packages may be considered using Partner and Collaboration Management (PCOM).</i> POPM.BP4: Define and monitor the project schedule. Schedule each activity of the project. Monitor the performance of the activities with respect to the schedule. POPM.BP5: Review progress of the activities. Regularly review the status and the fulfillment of the project's activities against estimated effort and duration. <i>Note 2: Progress for partnerships and collaborations based on goods and work packages may be considered individually using Partner and Collaboration Management (PCOM).</i> POPM.BP6: Manage the risks. Manage the risks to technical and organizational activities of the project. Ensure the impact of the risk treatment activities is monitored for the project. <i>Note 3: Activities may be affected by technical, economical, and schedule related risks.</i> <i>Note 4: Risk treatment options may include reduction, avoidance, transfer, or acceptance of risks.</i>

POPM.BP7: Analyze and monitor the organizational problems related to the project. Record, analyze and monitor the impact of the organizational problems related to the project.

Note 5: Organizational problems, as a type of non-technical problems, may be related to groups inside and outside the exemplary project, such as shared resources, internal service providers, central functions, etc. Examples of organizational problems are communication issues, lack of stakeholder involvement, insufficient skills identified at interfaces, etc.

Note 6: Resolution of organizational problems may be supported by Process Quality Assurance (PQAS), process improvement (e.g., as ISO/IEC TR 33014), or established management practices (e.g., lessons learned, inspect and adapt, retrospectives).

Potential Project Management	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5	Outcome 6	Outcome 7
Output Information Items							
08-56 Schedule				X	X		
14-10 Work package	X	X			X		
15-06 Project status				X	X	X	X
15-08 Risk analysis						X	
15-09 Risk status						X	
08-55 Risk treatment						X	
13-07 Problem							X
15-12 Problem status							X
14-02 Corrective action				X	X		
14-50 Stakeholder groups list			X				
Base Practices							
BP1: Identify, define, and estimate the activities	X						
BP2: Ensure technical feasibility	X	X					
BP3: Identify and monitor the project interfaces			X				
BP4: Define and monitor the project schedule				X			
BP5: Review progress of the activities			X	X	X		
BP6: Manage the risks						X	
BP7: Analyze and monitor the organizational problems related to the project							X

3.2 RTCM Release and Technical Configuration Management

Process ID
RTCM
Process name
Release and Technical Configuration Management
Process purpose
The purpose is to establish and maintain the integrity of engineering and product related work products of a process, to make them available to affected parties and to control the release of process outcomes.
Process outcomes
1) The engineering-related configuration items are identified. 2) The content for the release is defined. 3) The release is assembled from configured items. 4) Modifications and releases are made available to the affected parties. 5) Baselines are regularly recorded and controlled for the engineering-related configuration items. 6) The release documentation is defined and produced. 7) The product release is made available to the intended customer.

Base Practices
RTCM.BP1: Identify the engineering-related configuration items. Identify and document the engineering-related configuration items. RTCM.BP2: Control the modifications and releases. Establish mechanisms to control the configuration items, and control the modifications and releases using these mechanisms. <i>Note 1: Branch management may be used to manage complex software code.</i> RTCM.BP3: Establish baselines. Establish baselines for physical and logical integrity of the release, the related configuration items and for the delivery. RTCM.BP4: Define, assemble, and deliver the release. Identify the functionality to be included in each release according to the project schedule. Define the products associated with the release and build the release from configured items. Ensure that all documentation to support the release is produced, reviewed, approved and available. Deliver the release package to the intended customer.

Release and Technical configuration management	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5	Outcome 6	Outcome 7
Output Information Items							
01-52 Configuration item list	X						
11-04 Product release package		X	X			X	
13-06 Delivery evidence							X
13-08 Baseline					X		
14-01 Change history					X		
16-03 Configuration management system				X			
Base Practices							
BP1: Identify the engineering-related configuration items	X	X		X		X	
BP2: Control the modifications and releases		X		X	X		
BP3: Establish baselines					X		X
BP4: Define, assemble, and deliver the release		X	X			X	X

3.3 PQAS Process Quality Assurance

Process ID
PQAS
Process name
Process Quality Assurance
Process purpose
The purpose is to provide independent and objective assurance that the processes comply with the predefined provisions and that the non-conformances are resolved.
Process outcomes
1) Process quality assurance is performed independently and objectively without conflicts of interest. 2) Criteria for process quality assurance are defined. 3) Conformance of the process activities is verified, documented, and summarized. 4) Non-conformances of process activities are recorded, analyzed, and managed until closure. 5) An independent escalation mechanism is implemented.

Base Practices
PQAS.BP1: Establish independence and objectivity for process quality assurance. Ensure process quality can be assured objectively without conflict of interests resulting from dependencies within organizational structures. <i>Note 1: Organizational structures may be influenced by hierarchy or standardized process frameworks.</i> PQAS.BP2: Implement an escalation mechanism. Ensure that quality assurance can escalate problems independently to appropriate levels of the organization for resolution. PQAS.BP3: Define criteria to assure quality of the process activities. Define quality criteria for process activities and assure that the processes meet their defined goals according to the project schedule. Collect and analyze data of process quality assurance and initiate project-related actions. PQAS.BP4: Ensure the resolution of non-conformances. The deviations or non-conformances found in process quality assurance activities are recorded, analyzed, and managed until closure. PQAS.BP5: Summarize process quality assurance activities and results. Summarize activities, deviations, and trends of process quality assurance.

Process Quality Assurance	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5
Output Information Items					
13-19 Review evidence			X	X	
14-02 Corrective action				X	
16-50 Organizational structure	X				X
18-07 Quality criteria		X		X	
18-52 Escalation path					X
Base Practices					
BP1: Establish independence and objectivity for process quality assurance	X				
BP2: Implement an escalation mechanism					X
BP3: Define criteria to assure quality of the process activities		X			
BP4: Ensure the resolution of non-conformances			X	X	
BP5: Summarize process quality assurance activities and results			X		

3.4 TEPR Technical Problem Resolution

Process ID
TEPR
Process name
Technical Problem Resolution
Process purpose
The purpose is to ensure that technical problems are recorded, analyzed, and tracked to closure.
Process outcomes
1) The technical problems are recorded, analyzed, categorized, and assessed to identify an appropriate solution. 2) Technical problem resolution is initiated. 3) The technical problems are consistently tracked to closure. 4) The status of the technical problems and their trend are known.

Base Practices
TEPR.BP1: Record the technical problems, determine their cause and impact. Investigate the technical problems and determine their cause and impact to categorize the technical problems and to determine appropriate actions. <i>Note 1: Problem categorization may be based on severity, criticality (e.g., high, mid, low), or other criteria.</i> TEPR.BP2: Initiate technical problem resolution. Initiate appropriate actions to technically resolve the problems and include review of those actions. TEPR.BP3: Track the problems consistently to closure. Ensure the solution by tracking the status of problems to closure. <i>Note 2: The controlled resolution of problems may involve authorization of action(s), relationships, and dependencies (parent/child) and the adherence to schedule.</i> TEPR.BP4: Analyze problem trends. Collect and analyze the technical problem resolution management data and identify trends.

Technical Problem Resolution	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Output Information Items				
13-07 Problem	X	X	X	
15-12 Problem status			X	X
15-55 Problem analysis evidence	X			
Base Practices				
BP1: Record the technical problems, determine their cause and impact	X			
BP2: Initiate technical problem resolution		X		
BP3: Track the problems consistently to closure			X	
BP4: Analyze problem trends				X

3.5 SWDI Software Requirements, Design and Implementation

Process ID
SWDI
Process name
Software Requirements, Design and Implementation
Process purpose
The purpose is to have a structured and analyzed set of software requirements and a software architectural design available, that a software detailed design exists, and software units are constructed based on the detailed design.
Process outcomes
1) The software requirements are specified, analyzed, structured and prioritized. 2) A software architecture design is specified that identifies the components of the software and describes their interfaces and the dynamic interactions between the software components. 3) A detailed design is specified for each software component. 4) The software units are developed according to the software detailed design.

Base Practices
SWDI.BP1: Specify, analyze, structure and prioritize the software requirements. Specify, analyze and structure the functional and non-functional software requirements according to the defined characteristics for requirements. Prioritize the software requirements according to the project schedule. <i>Note 1: Software requirements can be structured, e.g., by categorizing, grouping, sorting, and prioritizing according to the project context.</i> SWDI.BP2: Specify and analyze the software architectural design. Specify and analyze the software architecture including components and their interfaces. Specify static and dynamic views of software architectural components. Determine and document the resource consumption objectives. SWDI.BP3: Specify the software detailed design. Specify the static and the dynamic aspects of the detailed design for each software component, including their interfaces, relationships and interactions between relevant software units. SWDI.BP4: Develop the software units. Develop and document the software units according to the software detailed design.

Software Requirements, Design and Implementation	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Output Information Items				
17-00 Requirement	X			
17-54 Requirement Attribute	X			
04-04 Software Architecture		X		
15-51 Analysis results	X	X		
04-05 Software Detailed Design			X	
11-05 Software Unit				X
Base Practices				
BP1: Specify, analyze, structure and prioritize the software requirements	X			
BP2: Specify and analyze the software architectural design		X		
BP3: Specify the software detailed design			X	
BP4: Develop the software units				X

3.6 SWIV Software Integration and Verification

Process ID
SWIV
Process name
Software Integration and Verification
Process purpose
The purpose is to verify the software units, to integrate the software and to ensure that the integrated software is consistent with its provisions and compliant with the software requirements.
Process outcomes
1) The verification measures for the software units, for software component integration and for software verification are specified. 2) The software units are verified with the specified verification measures, and the verification results are recorded. 3) The software components are integrated up to a complete integrated software, the integration is verified with the specified verification measures, and the verification results are recorded. 4) The integrated software is verified with the specified verification measures and the results of software verification are recorded. 5) Horizontal traceability is established on all levels.

Base Practices
SWIV.BP1 Specify and perform the unit verification measures. Specify and perform the software unit verification measures and record the verification results including pass/fail status. <i>Note 1: Examples for unit verification measures are static and dynamic analysis and code reviews.</i> SWIV.BP2 Specify and perform the verification measures for the integration. Specify and perform the verification measures for the integration and record the verification results including pass/fail status. Perform the integration of the software elements until the software is fully integrated. <i>Note 2: Examples for preconditions for starting integration can be successful software element verification or qualification of pre-existing software elements.</i> SWIV.BP3 Specify and perform the verification measures for software. Specify and perform the verification measures suitable to provide evidence of compliance of the integrated software with the software requirements. Record the verification results including pass/fail status. SWIV.BP4 Establish horizontal traceability. Ensure horizontal traceability from software requirements, software architecture and detailed design to corresponding verification measures and results. <i>Note 3: Horizontal traceability supports consistency, impact analysis and verification coverage demonstration for a respective V-model level.</i>

Software Integration and Verification	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5
Output Information Items					
08-60 Verification Measure	X				
08-58 Verification Measure Selection Set			X	X	
15-52 Verification Results		X	X	X	
01-03 Software Component			X		
01-50 Integrated Software				X	
13-51 Consistency Evidence					X
Base Practices					
BP1: Specify and perform the unit verification measures	X	X			
BP2: Specify and perform the verification measures for the integration	X		X		
BP3: Specify and perform the verification measures for software	X			X	
BP4: Establish horizontal traceability					X

3.7 REEL Requirements Elicitation

Process ID
REEL
Process name
Requirements Elicitation
Process purpose
The purpose is to gather and process the stakeholder needs and requirements of the exemplary product or service.
Process outcomes
1) Exchange of the stakeholder expectations is established. 2) The stakeholder requirements are agreed. 3) Stakeholder needs are monitored continuously. 4) Evolving stakeholder requirements are continuously evaluated.

Base Practices
REEL.BP1: Obtain the stakeholder expectations and requests. Obtain and define the stakeholder expectations and requests through direct solicitation of stakeholder input and other sources containing inputs to the stakeholder requirements, considering the target operating and hardware environment. <i>Note 1: Requirements elicitation may involve project partners up and downstream.</i> REEL.BP2: Agree on the requirements. Formalize the stakeholder's expectations and requests into requirements. Reach a common understanding of the set of stakeholder requirements among the affected parties by obtaining an explicit agreement from all affected parties. <i>Note 2: Reviewing the requirements and requests with the stakeholder supports a better understanding of stakeholder needs and expectations.</i> <i>Note 3: The agreed stakeholder requirements may be influenced by feasibility studies, effort and schedule impact analysis.</i> REEL.BP3: Analyze the changes on stakeholder requirements. Analyze all changes made to the agreed stakeholder requirements. Assess the impact and risks of the resulting modification. <i>Note 4: Accepted stakeholder change requests may be followed up by Technical Change Request Management (TCRM).</i>

REEL Requirements Elicitation	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Output Information Items				
15-51 Analysis Results				X
17-00 Requirement	X	X		
17-54 Requirement Attribute		X	X	X
Base Practices				
BP1: Obtain the stakeholder expectations and requests	X			
BP2: Agree on the requirements		X		
BP3: Analyze the changes on stakeholder requirements			X	X

3.8 SYRD System Requirements and Design

Process ID
SYRD
Process name
System Requirements and Design
Process purpose
The purpose is to have a structured and analyzed set of system requirements and a system architectural design available.
Process outcomes
1) The system requirements are specified, analyzed, structured, and prioritized. 2) A system architecture design is specified that identifies the elements of the system and describes their interfaces and the dynamic interactions of the system elements.

Base Practices
SYRD.BP1: Specify, analyze, structure and prioritize the system requirements. Specify, analyze and structure the functional and non-functional system requirements according to the defined characteristics for requirements. Prioritize the system requirements according to the project schedule. <i>Note 1: System requirements can be structured, e.g., by categorizing, grouping, sorting, and prioritizing according to the project context.</i> <i>Note 2: For changes to the stakeholder's requirements, Technical Change Request Management (TCRM) may apply.</i> <i>Note 3: The analysis of impact on effort and schedule supports the adjustment of project estimates. Refer to Potential Project Management (POPM).</i> SYRD.BP2: Specify and analyze the system architectural design. Specify and analyze the system architecture including system elements and their interfaces. Specify static and dynamic views of system elements.

SYRD System Requirements Analysis and Design			Outcome 1	Outcome 2
Output Information Items				
17-00 Requirement			X	
17-54 Requirement Attribute			X	
04-06 System Architecture				X
15-51 Analysis Results			X	X
Base Practices				
BP1: Specify, analyze, structure and prioritize the system requirements			X	
BP2: Specify and analyze the system architectural design				X

3.9 SYIV System Integration and Verification

Process ID
SYIV
Process name
System Integration and Verification
Process purpose
The purpose is to integrate the system and to ensure that the integrated system is consistent with its provisions and compliant with the system requirements.
Process outcomes
1) The verification measures for system integration and for system verification are specified. 2) The system elements are integrated up to a complete integrated system, the integration is verified with the specified verification measures, and the verification results are recorded. 3) The integrated system is verified with the specified verification measures, and the results of system verification are recorded. 4) Horizontal traceability is established on all levels.

Base Practices
SYIV.BP1: Specify and perform the verification measures for integration. Specify and perform the verification measures for the integration and record the verification results including pass/fail status. Perform the integration of the system elements until the system is fully integrated. <i>Note 1: Examples for preconditions for starting integration can be successful system element verification or qualification of pre-existing system elements.</i> SYIV.BP2: Specify and perform the system verification measures. Specify and perform the verification measures suitable to provide evidence of compliance of the integrated system with the system requirements. Record the verification results including pass/fail status. SYIV.BP3: Establish horizontal traceability. Ensure horizontal traceability from the system requirements and the system architecture to the corresponding verification measures and results. <i>Note 2: Horizontal traceability supports consistency, impact analysis and verification coverage demonstration for a respective V-model level.</i>

SYIV System Integration and Verification	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Output Information Items				
08-60 Verification Measure	X			
08-58 Verification Measure Selection Set		X	X	
15-52 Verification Results		X	X	
13-51 Consistency Evidence				X
11-06 Integrated System		X		
Base Practices				
BP1: Specify and perform the verification measures for integration	X	X		
BP2: Specify and perform the system verification measures for system	X		X	
BP3: Establish horizontal traceability				X

3.10 MLEG Machine Learning Engineering

Process ID
MLEG
Process name
Machine Learning Engineering
Process purpose
The purpose is to specify the requirements (for an ML model and corresponding ML data), and to provide a trained, validated, tested and deployed ML model.
Process outcomes
1. The requirements for the ML model and the data requirements are documented 2. The data for training, validation and testing is appropriately structured 3. The defined ML model is trained and validated with the corresponding data sets 4. The release candidate is tested with the ML test data set

Base Practices
MLEG.BP1: Specify ML requirements and ML data requirements. Specify, analyze, structure and prioritize ML requirements and ML data requirements. This includes functional and non-functional requirements for the ML model as well as data requirements. <i>Note 1: The ML data requirements are input for MLDM Machine Learning Data Management and MLEG Machine Learning Engineering process.</i> <i>Note 2: Nonfunctional requirements may include relevant characteristics of the ODD and KPIs as robustness, performance, level of trustworthiness, and include criteria for the ML architecture.</i> MLEG.BP2: Specify and structure data for training, validation and testing. Ensure that data is provided and appropriately structured. The data for training and validation should be separated from data for testing. <i>Note 3: Using an independent data set to avoid overfitting, the testing data shall be used to test the ML model against the requirements.</i> MLEG.BP3: Perform training and validation of the defined ML model. Ensure an appropriate training environment, Train and validate the model using an appropriate set of data. <i>Note 4: The validation shall be used to show that the model covers the requirements to an extent to continue with testing.</i> MLEG.BP4: Perform testing of the deployed model. Perform testing of the deployed model prior to delivery in target environment, using an appropriate set of data.

MLEG Machine Learning Engineering	Outcome 1	Outcome 2	Outcome 3	Outcome 4
17-00 Requirement	X			
17-54 Requirement attribute	X			
03-51 ML data set		X		
01-53 Trained ML model			X	
13-50 ML test results			X	X
11-50 Deployed ML model				X
BP1: Specify ML requirements and ML data requirements	X			
BP2: Specify and structure data for training, validation and testing		X		
BP3: Perform training and validation of the defined ML model			X	
BP4: Perform testing of the deployed model				X

3.11 MLDM Machine Learning Data Management

Process ID
MLDM
Process name
Machine Learning Data Management
Process purpose
The purpose is to define and align ML data with ML data requirements, maintain the integrity and quality of the ML data.
Process outcomes
1. An ML data management system including an ML data lifecycle is established. 2. The ML data quality approach is developed including ML data quality criteria. 3. The collected ML data are processed based on ML data requirements. 4. The ML data are verified against defined ML data quality criteria.

Base Practices
MLDM.BP1: Establish an ML data management system Establish an ML data management system which supports • <i>ML data management labelling/annotation and structuring</i> • <i>ML data life cycle including a status model</i>
MLDM.BP2: Develop a quality approach for ML data. Develop a quality approach including the ML data quality criteria for ML data based on ML data requirements. <i>Note 1: Examples of ML data quality criteria are relevant data sources, reliability and consistency of labelling, completeness against ML data requirements.</i> <i>Note 2: The ML data management system shall support the quality criteria and activities of the ML data quality approach.</i>
MLDM.BP3: Process the collected ML data The collected raw data are processed (annotated, analyzed and structured) according to the ML data requirements. Relevant sources for raw data are identified and continuously monitored for changes. <i>Note 3: Continuous monitoring should include the ODD and may lead to changes of the ML requirements.</i>
MLDM.BP4: Assure the quality of ML data. Perform the activities according to the ML data quality approach to ensure that the ML data meet the defined ML data quality criteria <i>Note 4: These activities may include sample-based reviews or statistical methods</i>

MLDM Machine Learning Data Management	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Output Information Items				
16-52 ML data management system	X			
19-50 ML data quality approach		X		
03-53 ML data			X	X
Base Practices				
BP1: Establish an ML data management system	X			
BP2: Develop and apply quality criteria for ML data		X		
BP3: Process the collected ML data			X	
BP4: Assure the quality of ML data				X

3.12 PCOM Partner and Collaboration Management

Process ID
PCOM
Process name
Partner and Collaboration Management
Process purpose
The purpose is to select partners and collaborations according to relevant criteria and to monitor their performance against agreed commitments.
Process outcomes
1) The evaluation criteria for partners and collaborations are established. 2) The partners and collaborations are evaluated against the defined criteria. 3) The joint activities are agreed. 4) The performance of the partners and collaborations is monitored against the agreements.

Base Practices
PCOM.BP1: Establish evaluation criteria. Analyze the relevant requirements to define evaluation criteria for capabilities of partners and collaborations. <i>Note 1: Criteria may consider commercial constraints, quality requirements, technical evaluation and capabilities required for norm and standard conformance (such as conformance to norms of safety, cybersecurity, and other technical norms).</i> PCOM.BP2: Evaluate the partners and collaborations against the defined criteria. Collect information about the capabilities of the partners and collaborations and evaluate it against the established evaluation criteria. <i>Note 2: The evaluation may be supported by audit and assessment results, certifications, policies, financial reports, technical demonstration, portfolio reviews, roadmap information, historical data, etc.</i> PCOM.BP3: Agree on joint activities. Establish an agreement on joint activities, type and frequency of joint activities and reviews. <i>Note 3: Agreements may include ownership of processes, type and frequency of joint activities, failure management and reviews.</i> PCOM.BP4: Review the performance of the partners and collaborations. Review the progress of the collaborations and partnerships regarding schedule, quality, and effort on the agreed regular basis. Agree on corrective actions accordingly.

Partner and Collaboration Management	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Output Information Items				
18-50 Supplier evaluation criteria	X			
15-21 Supplier evaluation		X		
15-51 Analysis results		X		X
02-01 Commitment/agreement			X	X
02-50 Interface agreement		X	X	
13-14 Progress status				X
14-02 Corrective action				X
Base Practices				
BP1: Establish evaluation criteria	X			
BP2: Evaluate the partners and collaborations against defined criteria		X		
BP3: Agree on joint activities			X	
BP4: Review the performance of the partners and collaborations				X

3.13 TCRM Technical Change Request Management

Process ID
TCRM
Process name
Technical Change Request Management
Process purpose
The purpose is to ensure that the technical change requests are analyzed, tracked, and implemented.
Process outcomes
1) The technical change requests are analyzed, the dependencies and relationships to other technical change requests are identified, and the impact is estimated. 2) The implementation of technical change requests is confirmed. 3) The status of all technical change requests is known, and the technical change requests are tracked to closure.

Base Practices
TCRM.BP1: Analyze and assess the technical change requests. The technical change requests are analyzed by relevant parties according to the analysis criteria. The work products affected by the change requests and the dependencies on other technical change requests are determined. The impact of the technical change requests is assessed. <i>NOTE 1: Examples for analysis criteria are: resource requirements, scheduling issues, risks, benefits, etc.</i> TCRM.BP2: Confirm the implementation of the technical change requests. The implementation of the technical change requests is confirmed before closure by relevant stakeholders. TCRM.BP3: Track the technical change requests to closure. The status of the technical change requests is known, and they are tracked to closure.

Technical Change Request Management			
	Outcome 1	Outcome 2	Outcome 3
Output Information Items			
13-16 Change request	X	X	X
18-57 Change analysis criteria	X		
Base Practices			
BP1: Analyze and assess the technical change requests	X		
BP2: Confirm the implementation of the technical change requests		X	
BP3: Track the technical change requests to closure			X

3.14 CSGE Cybersecurity Goal Elicitation

Process ID
CSGE
Process name
Cybersecurity Goal Elicitation
Process purpose
The purpose is to derive cybersecurity goals and to ensure traceability between the cybersecurity risk assessment and the cybersecurity goals.
Process outcomes
1) The threats are analyzed and the cybersecurity risks evaluated. 2) Cybersecurity risk treatment options are determined. 3) The cybersecurity goals are defined for risk reduction and avoidance. 4) Traceability is established between the cybersecurity goals and the threat scenarios.

Base Practices
CSGE.BP1: Analyze the threats and evaluate the cybersecurity risks. Analyze the threats to determine the attack paths that are relevant for the project. Evaluate relevant threat scenarios for their impact, severity and likelihood for respective project life cycle phases and stakeholders. <i>Note 1: Analysis may be for relevance to financial, safety, privacy, and operational terms.</i> CSGE.BP2: Define cybersecurity risk treatment options. For each cybersecurity risk, define the selected treatment option to reduce, avoid, accept or transfer (share) the risks. <i>Note 2: Accepted and transferred (shared) risks can define cybersecurity claims that may require rationale and justification.</i> <i>Note 3: Risks may be handled individually or as a set of risks.</i> CSGE.BP3: Derive and align the cybersecurity goals for risk reduction and avoidance. Derive the cybersecurity goals for the threat scenarios that were chosen for reduction and avoidance, and align possible conflicts with established cybersecurity goals. CSGE.BP4: Establish traceability between the cybersecurity goals and the threat scenarios. <i>Note 4: Traceability supports consistency and facilitates impact analyses.</i>

Cybersecurity Goal Elicitation	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Output Information Items				
17-53 Cybersecurity threat scenario	X			
15-08 Risk analysis	X	X		
08-55 Risk treatment		X	X	
17-51 Cybersecurity goals			X	
13-51 Consistency Evidence				X
Base Practices				
BP1: Analyze the threats and evaluate the cybersecurity risks	X			
BP2: Define cybersecurity risk treatment options		X		
BP3: Derive and align the cybersecurity goals for risk reduction and avoidance			X	
BP4: Establish traceability between the cybersecurity goals and the threat scenarios				X

3.15 CSVV Cybersecurity Verification and Validation

Process ID
CSVV
Process name
Cybersecurity Verification and Validation
Process purpose
The purpose is to specify and verify the cybersecurity requirements, and to validate the cybersecurity goals.
Process outcomes
1) Cybersecurity requirements are derived from the cybersecurity goals. 2) Risk treatment verification is specified and performed. 3) The activities are identified and documented to validate cybersecurity goals, and validation results are recorded. 4) Traceability is established between the cybersecurity goals and the validation results. 5) Traceability is established between the cybersecurity requirements and goals, and between the cybersecurity requirements and the risk treatment verification specification.

Base Practices
CSVV.BP1: Specify the cybersecurity requirements for the cybersecurity goals. Specify the functional cybersecurity requirements for the cybersecurity goals, including criteria for the achievement of the cybersecurity goals. <i>Note 1: This may include requirements for post-development phases such as preproduction, production, operation, maintenance, and decommissioning.</i> CSVV.BP2: The cybersecurity verification measures are specified and performed. Specify and perform the verification measures suitable to provide evidence for compliance of the integrated system with the cybersecurity requirements. Record the verification results including pass/fail status. <i>Note 2: Depending on the context the system might be a pure software system.</i> CSVV.BP3: The cybersecurity validation activities are identified and documented. The cybersecurity validation activities are identified and documented to validate the cybersecurity goals. CSVV.BP4: The results of the cybersecurity validation activities are recorded. CSVV.BP5: Traceability is established. Ensure traceability between the cybersecurity requirements and goals and between the cybersecurity requirements and the risk treatment verification specification. Ensure traceability between the cybersecurity goals and the validation results. <i>Note 3: Traceability supports consistency, verification, and validation coverage demonstration.</i>

Cybersecurity Verification and Validation	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5
Output Information Items					
17-00 Requirement	X				
08-60 Verification Measure		X			
08-58 Verification Measure Selection Set		X			
13-19 Review evidence					X
15-51 Analysis Results					X
15-52 Verification Results		X			
13-24 Validation Results				X	
08-59 Validation Measure			X		
Base Practices					
BP1: Specify the cybersecurity requirements for the cybersecurity goals	X				
BP2: The cybersecurity verification measures are specified and performed		X			
BP3: The cybersecurity validation activities are identified and documented			X		
BP4: The results of the cybersecurity validation activities are recorded				X	
BP5: Traceability is established					X

4 Consistency and traceability

The Automotive SPICE® Potential Analysis includes reduced requirements for consistency and traceability in favor of efficiency and more relevant aspects.

4.1 Consistency and traceability within System Level and Software Level plugins

The System Level and Software Level plugins include the processes Software Requirements, Design and Implementation (SWDI), Software Integration and Verification (SWIV), System Requirements Analysis and Design (SYRD) and System Integration and Verification (SYIV). Within the Automotive SPICE® Potential Analysis, the completeness of work breakdown is not checked, and therefore vertical traceability cannot be evaluated. Instead, the effective horizontal traceability is inspected for every single logical layer.

The difficulty to evaluate the completeness of vertical traceability during the ASPICE PoA is in no way an endorsement to dismiss the necessity of establishing vertical traceability as an effective means to ensure consistency between requirements and designs in any development. Any inconsistency identified within a coherent scope shall still be seen as a weakness in specifying and analyzing requirements and designs.

The direct horizontal traceability shown shall not be interpreted as a requirement for strictly direct and granular traceability, as consistency may also be established with a suitable chain of other elements if they are adequate and comparable for their purpose and intent.

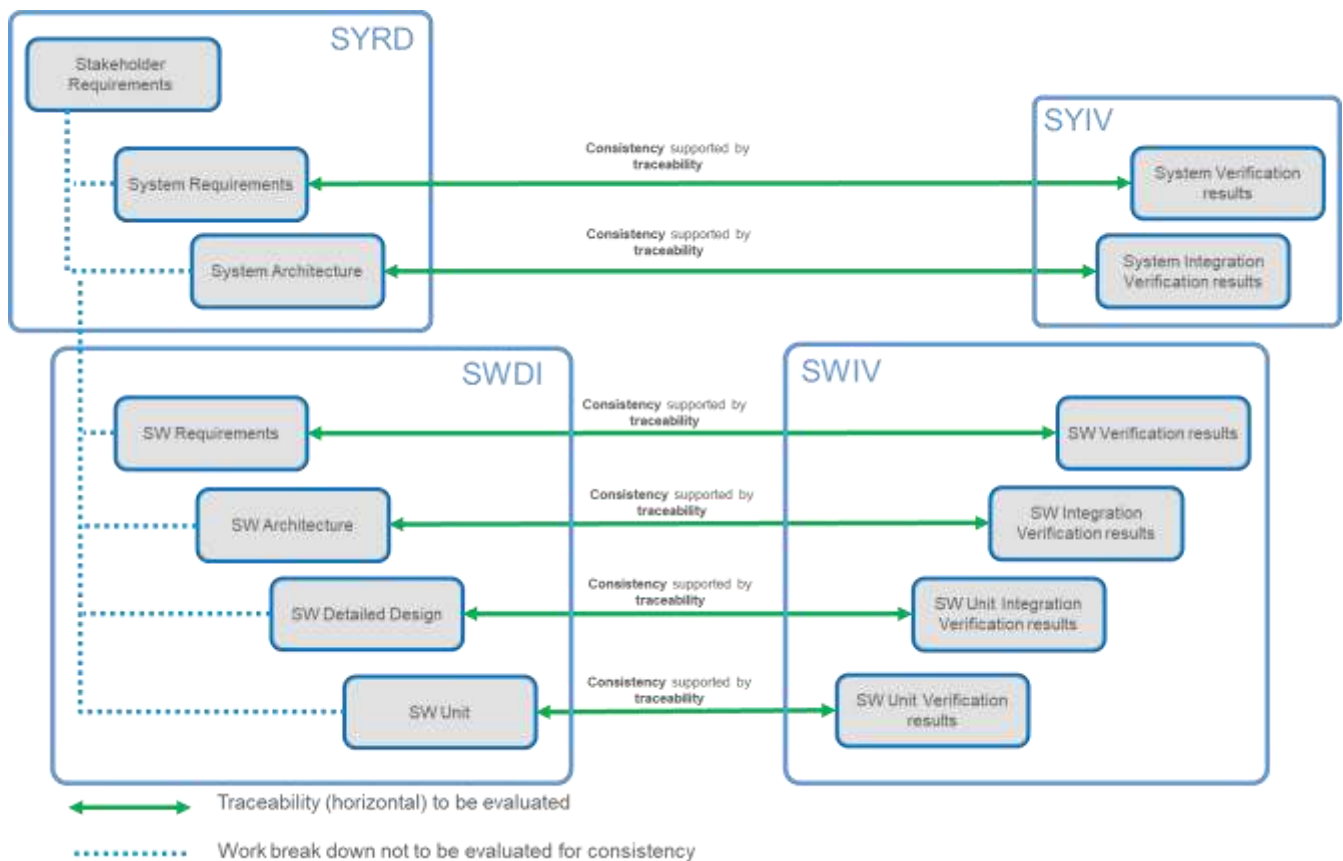


Figure 9 — Traceability and consistency within System Level and Software Level plugins

4.2 Relationships and traceability of Cybersecurity

The processes Cybersecurity Goal Elicitation (CSGE) and Cybersecurity Verification and Validation (CSVV) add cybersecurity aspects to the Automotive SPICE® Potential Analysis. The following picture provides an overview of the major elements, work products and information items. It shows the add-on character of Cybersecurity Verification and Validation (CSVV), which requires the performance of at least System Level or Software Level plugin illustrated exemplarily as V-model in Figure 10.

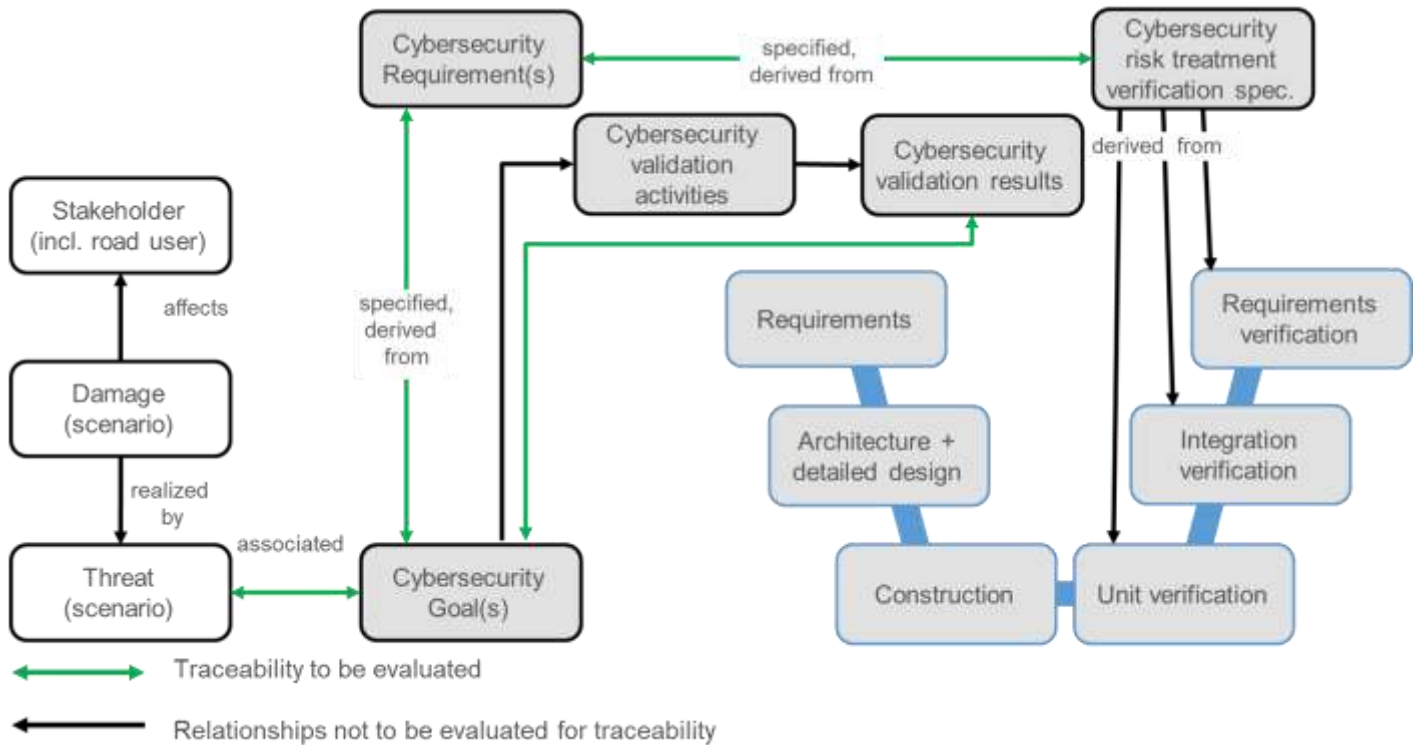


Figure 10 — Traceability and relationships of Cybersecurity

5 Guideline

The Automotive SPICE® Potential Analysis aims to simplify assessments by limiting redundancy and dependencies between the evaluation of different processes. As a consequence, results shall be noted only once when indicated within one process. For example, in Figure 11 the top-level process relation is within Technical Problem Resolution (TEPR), a resulting finding for it should then be noted to Technical Problem Resolution (TEPR) only and must not be noted redundantly within Technical Change Request Management (TCRM).

The Automotive SPICE® Potential Analysis therefore does not provide any guidance to dependencies or rules between processes.

Rules for rating consistency between BPs are not defined for processes within the Automotive SPICE® Potential Analysis, due to the nature of BPs as describing separate concerns.

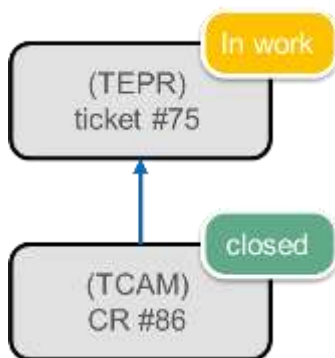


Figure 11 — Example of work products involving 2 different processes

5.1 POPM Potential Project Management

The purpose is to identify and manage the activities of an exemplary project to develop a product, manage the risks and monitor the organizational problems related to the project.

5.1.1 General Information

The evaluation of the Potential Project Management within the Automotive SPICE® Potential Analysis does not include completeness for work packages of the exemplary project and relates to the observable activities that have been identified, defined, and performed instead.

5.1.1.1 Resources

As the focus of an Automotive SPICE® Potential Analysis is on a potential project setting yet to be confirmed, the individual resources within the evaluated organization unit are more likely to change later, may include a high number of irrelevant functions, and therefore cannot be evaluated.

The focus is shifted from the evaluation of actual planning, deployment, and management of resources to the definition and monitoring of activities, which can be more readily evaluated within a potential project. This influences also feasibility, described further below.

See Rationale *RAG.1 “Resources”*.

5.1.1.2 Scope of work and project life cycle

Since the exemplary project(s) in an Automotive SPICE® Potential Analysis could be significantly different to the potential project settings (customer, organization, technology, product, market, regulations, etc.), details in **scope of work** and **project life cycle** specific to the exemplary project(s)

does not necessarily infer success in the potential project. The focus is instead placed on the practical aspects of the project **activities** and **schedule**.

See Rationale *RAG.2 “Scope of work”*.

5.1.1.3 Feasibility

Feasibility in an Automotive SPICE® Potential Analysis is restricted to time, schedule, effort, and technical feasibility. Other aspects, for example related to resources, skills and work split opportunities, as presented in Rationale *RAG.1 “Resources”*, are not to be evaluated with the Automotive SPICE® Potential Analysis.

See Rationale *RAG.3 “Feasibility”*.

5.1.1.4 Responsibilities

Accepting that the organizational setting and the qualification and assignment of resources to roles and responsibilities in the potential project could differ from those in the exemplary project, the focus of the Automotive SPICE® Potential Analysis is on interfaces instead of individual roles and responsibilities.

See Rationale *RAG.4 “Responsibilities”*.

5.1.1.5 Risks

Risk management is included in the scope of the Potential Project Management (PPM) process. Only the management of available risks is to be evaluated, while their identification is out of scope.

See Rationale *RAP.3 “Risk identification”*.

5.1.2 Rating rules within the process

[PPM.RL.1] If the estimation approach used and the origin of the estimates for activities are not reasonable, the indicator BP1 shall not be rated Green.

[PPM.RL.2] If the dependencies between activities are not identified, the indicator BP1 shall not be rated Green.

[PPM.RL.3] If the progress of activities is not systematically measured, the indicator BP5 shall not be rated Green.

[PPM.RL.4] If links between different activities are not supported by tools, this shall not be used to downrate the indicators BP4 or BP5 respectively.

[PPM.RL.5] If the definition of activities and schedule(s) does not sufficiently reflect risk treatment activities, the indicator BP6 shall not be rated Green.

5.2 RTCM Release and Technical Configuration Management

The purpose is to establish and maintain the integrity of engineering and product related work products of a process, to make them available to affected parties and to control the release of process outcomes.

5.2.1 General Information

Within the Automotive SPICE® Potential Analysis, the Release and Technical Configuration Management (RTCM) evaluates primarily engineering related configuration items (see *RAP.9 "Configuration items"*). It covers the identification of configuration items and the control of modifications required to fulfill the engineering-related activities.

Consequently, the focus on technical aspects limits the baseline evaluation, as described in *RAP.10 "Baseline completeness and consistency"*.

While Process Quality Assurance (PQAS) evaluates process related mechanisms and criteria to ensure work product quality, the actual conditions of work products for a release shall be evaluated in Release and Technical Configuration Management (RTCM).

5.2.2 Rating rules within the process

5.2.2.1 Define, build, and deliver the release

In product development the agreed functional content results in a release, which may include viable, inspectable work items and documentation. The Automotive SPICE® Potential Analysis evaluates the creation, assembly, documentation, and delivery of such releases, which should be consistent with the project schedule according to *RAG.2 "Scope of work"*.

The sequence of implementing these functionalities is substantiated in the definition of the release scope which is part of Potential Project Management (POPM).

[RTCM.RL.1] If the functionality of the release is not identified according to the project schedule, the indicator BP4 shall not be rated Green.

5.3 PQAS Process Quality Assurance

The purpose is to provide independent and objective assurance that the processes comply with the predefined provisions and that the non-conformances are resolved.

5.3.1 General Information

Process Quality Assurance (PQAS) may use quality relevant methods such as reviews, audits, assessments, workshops to assure processes are conforming to provisions. Agile methods in development may also demonstrate suitable quality assurance measures which may overlap or even substitute such methods. Examples of agile principles are “early and objective evaluation”, definition of done (DoD), retrospective meeting and integrated learning cycles.

Activities within processes should be assured to comply with their provisions as a minimum with respect to the scope of the available project schedule, see also the limitation of *RAG.2 “Scope of work.”*

Process Quality Assurance (PQAS) in the Automotive SPICE® Potential Analysis should be reviewed only for non-conformances that are within the scope of the instance under review. Non-conformances that are solved in other process levels, such as organizational changes raised by the evaluation of the Potential Project Management (POPM) process, shall not be reflected or evaluated for the Process Quality Assurance (PQAS) in alignment with *RAP.23 “Cross relationships”*.

Since the PQAS focusses on process quality only, the quality assurance of work products shall have a very limited scope within the assessment. Of course, all quality activities should have the goal of improving the results of the processes and need to be rated as such. Especially work product reviews are a good practice in this field. While they should be considered in the ASPICE Potential Analysis, they may only be analyzed to understand the systematic approach.

As the actual statuses of work products for a release shall be evaluated in Release and Technical Configuration Management (RTCM), the focus of Process Quality Assurance (PQAS) in comparison is to check the existence of mechanisms and criteria to ensure work product quality.

5.3.2 Rating rules within the process

5.3.2.1 Independence, objectivity and escalation in quality assurance

Independence aids quality assurance to perform its activities without conflicts of interest and free from bias. Evaluation of independence requires the review of the organizational structure or the structure of the given process framework. Within small organizations people may have close relationships with each other, reducing the overall achievable level of independence. Independence shall therefore be evaluated relative to the overall achievable level.

An escalation mechanism shall be in place to ensure non-conformities can be addressed to an appropriate level within the organization, e.g., when those can't be solved within the project team. This can be supported by mechanisms specific to respective organizations within the company, for example top level board presentation, task force, or a workshop. Criteria of urgency and impact may help to identify the appropriate level of management and to facilitate preparation of decision opportunities.

The frequency of escalations may influence its evaluation. A frequently used escalation may implicitly substitute a regular problem resolution process. On the other hand, an escalation which is never used can be difficult to evaluate in terms of effectiveness and may only be evaluated based on its process documentation.

[PQAS.RL.1] If escalations are not followed up by effective corrective actions, the indicator BP2 shall be rated Red.

5.3.2.2 Define criteria to assure quality of process activities

Process Quality Assurance (PQAS) should identify and define project- and context-specific criteria to suit the needs of process conformance. This may include for example timing, budget, customer quality criteria, regulatory or guideline conformance, accuracy, auditability, etc.

Process Quality Assurance (PQAS) activities shall at least verify compliance with processes related to the available project schedule. Relevant criteria may be assured within activities also by including process assessments, lessons learned, retrospective results and regular checks of methods, tools, and document handling.

[PQAS.RL.2] If the defined quality criteria are not followed up in their respective processes, the indicator BP3 shall be rated Red.

[PQAS.RL.3] If the quality assurance of process activities is based on performing process assessments (either by a customer or internally) only, the indicator BP3 shall be rated Red.

5.3.2.3 Ensure resolution of non-conformances

Non-conformances must be resolved within an appropriate timeframe. This can include ad-hoc corrective actions as well as solutions requiring more effort and further stakeholders. Non-conformances should be recorded, analyzed, and managed until they get closed.

[PQAS.RL.4] If existing non-conformances related to process activities are neither identified nor documented, the indicator BP4 shall not be rated Green.

[PQAS.RL.5] If existing non-conformances are not tracked or not resolved in a timely manner, the indicator BP4 shall not be rated Green.

5.4 TEPR Technical Problem Resolution Management

The purpose is to ensure that technical problems are recorded, analyzed, and tracked to closure.

5.4.1 General Information

Technical Problem Resolution Management (TEPR) covers the management of technical issues where more than one stakeholder is involved, or which are not resolved immediately.

The Automotive SPICE® Potential Analysis Technical Problem Resolution Management (TEPR) can only consider problems that are rooted in technical problems and initiate at least one technical solution. Other problem types shall only be evaluated in Automotive SPICE® Potential Analysis in the processes where they are directly found and managed, e.g., Potential Project Management (PPM). See *RAP.23 “Cross relationships”*.

5.4.1.1 Recording of technical problems

Technical problems shall include sufficient information to:

- Ensure project related traceability, such as project name, version or samples they were identified in, or initiator of the problem.
- Allow unique identification of each of them, e.g., by numbering or naming.
- Document the circumstances and effects of them, at least to the initiator.

5.4.1.2 Analysis and categorization of technical problems

Technical problems must be analyzed for their potential effects on the system/software/hardware and the work products that are affected, such as designs, requirements, or specifications.

Categorization depends on the overall number of technical problems and may use different characteristics to sort and filter in order to manage them. Such can be made for severity, criticality, urgency of required solution, as well as criteria like functional classes, subject matter domains or individuals of a team.

5.4.1.3 Problem resolution and parallel work

Technical problems may be solved by one or many technical solutions, which may create parallel work activities. For example, problems can be linked to other problems, or have parent/child relations or relationships to other tasks. The status and information of related problem tickets shall be consistent throughout the whole problem resolution process. Inconsistencies with other process tasks or tracking items shall be noted and considered in the rating. Figure 12 gives examples for this where either sub-problems or sub-tasks are still under work when the original problem ticket is already marked as “resolved”.

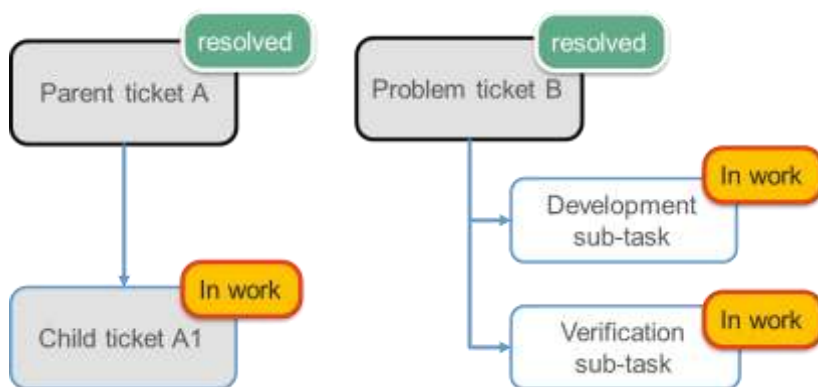


Figure 12 — Examples of inconsistent parallel work items

5.5 SWDI Software Requirements, Design and Implementation

The purpose is to have a structured and analyzed set of software requirements and a software architectural design available, that a software detailed design exists, and software units are constructed based on the detailed design.

5.5.1 General Information

Software Requirements, Design and Implementation (SWDI) covers all software related requirement, design, and implementation activities.

The software requirements (both functional and non-functional) are satisfied by the design solutions which are specified in the software architecture. Requirement analysis and architectural design need not be strictly sequential. Design decisions made in the software architecture and the detailed design may lead to iterative rework in software requirements, and vice versa.

5.5.1.1 Iterative vs. incremental development

Usually, the functional content in the product changes iteratively and evolves incrementally across releases. The term “increment” can be understood as adding a feature or element that did not exist before (analogy: building a house). The term “iteration” can be understood as refining, or adapting, an existing feature or element (analogy: a sculptor working on a sculpture).

Therefore, the complete set of requirements of the final product does not necessarily have to be available at the start of the project. Rather, release scopes agreed with the customer will define increments and iterative rework. In this respect, requirement creation can be driven by release definitions over time.

5.5.1.2 Structuring and prioritization of requirements

A possible and typical approach to prioritizing requirements is the allocation of requirements to releases. Since the scope of the Automotive SPICE® Potential Analysis may be different to the intended future project scope, prioritization is limited to the set of requirements related to the available project schedule. See *RAP.21 “Prioritization of requirements”*.

Further ways of structuring requirements may be realized by using attributes in tools for categorization, or a hierarchical headline structure with an adequate depth.

5.5.2 Rating Rules within the process

5.5.2.1 Specification of software requirements

[SWDI.RL.1] If different approaches of documenting requirements are used concurrently (e.g., Word processor file, Application Lifecycle Management tool, database), the indicator BP1 shall not be downrated.

5.5.2.2 Analysis of software requirements

[SWDI.RL.2] If analysis results of requirements are not demonstrated by separate analysis reports or review records but by means of attributes, commenting etc., the indicator BP1 shall not be downrated.

5.5.2.3 Structuring of software requirements

[SWDI.RL.3] If the notions “functional” and “non-functional” are not used as a structuring, categorization, or classification criterion, the indicator BP1 shall not be downrated.

5.5.2.4 Prioritization of software requirements

[SWDI.RL.4] If there is no evidence for prioritization but there is a separate release plan consistently mapping software functionality to future releases, the indicator BP1 shall not be downrated.

5.5.2.5 Specification of software architecture

[SWDI.RL.5] If component interfaces are specified in the detailed design, the indicator BP2 shall not be downrated.

5.5.2.6 Analysis of software architecture

[SWDI.RL.6] If resource consumption objectives are missing, the indicator BP2 shall not be rated Green.

5.5.2.7 Specification of software detailed design

[SWDI.RL.7] If the detailed design does not define interfaces, the indicator BP3 shall not be rated Green.

5.5.2.8 Implementation of software unit

[SWDI.RL.8] If the unit implementation is not based on a software detailed design, the indicator BP4 shall not be rated Green.

5.6 SWIV Software Integration and Verification

The purpose is to verify the software units, to integrate the software and to ensure that the integrated software is consistent with its provisions and compliant with the software requirements.

5.6.1 General Information

Verification of software within the Automotive SPICE® Potential Analysis includes the level of software unit verification and their integration up to the level of software representing the intended functionality of software requirements.

Some software-related verification levels can be given more focus and higher depth for verification coverage than others, which may strategically be derived from the respective software product type. For example, software products that are to be further integrated into other software may focus highly on software unit, architecture, and design level integration and less on SW requirements verification level.

Complexity and the number of verification measures depend also on the variants for which the software product may be configured. The Software Integration and Verification (SWIV) process should be evaluated only for a single, exemplary variant (*RAP.22 “Select verification measures”*) related to the available project schedule (*RAG.2 “Scope of work”*).

5.6.1.1 Traceability and consistency

See chapter 4 for details on the consistency and traceability within the Automotive SPICE® Potential Analysis.

5.6.2 Rating Rules within the process

5.6.2.1 Definition of verification measures

[SWIV.RL.1] If entry/exit criteria are reasonably specified for a set of verification measures instead of each individual verification measure, the indicators BP1, BP2 and BP3 shall not be downrated.

5.6.2.2 Automation of verification measures

[SWIV.RL.2] If a verification measure is automated and the correctness, completeness and consistency of the corresponding scripts and programs are not addressed in the verification measure definition, the affected indicators BP1, BP2 or BP3 shall not be rated Green.

5.6.2.3 Exploratory testing

The state-of-the-art testing not only comprises testing derived from requirements, but also exploratory testing based on experience, such as “error guessing based on knowledge”. This is valuable as it adds to the quality of the product. Therefore, exploratory tests that are based on experience cannot be traced or demonstrated to be consistent with the software requirements by definition. Nevertheless, traceability is still needed between exploratory test cases and their results.

Notwithstanding the benefits, in principle exploratory testing alone cannot provide reliable and conclusive evidence of verification of the software against the relevant specifications, which is often required from a standard, regulatory or customer perspective.

[SWIV.RL.3] If explorative tests used as verification measures do not have traceability to software requirements, software architecture or software detailed design, the indicator BP4 shall not be downrated.

5.7 REEL Requirements Elicitation

The purpose is to gather and process the stakeholder needs and requirements of the exemplary product or service.

5.7.1 General Information

Requirements elicitation is a very important aspect of every business relationship since stakeholder satisfaction is conditioned by understanding stakeholder needs and desires.

Selecting the Requirements Elicitation (REEL) process in the scope of an Automotive SPICE® Potential Analysis is recommended in most cases. It shall give an overview of how the stakeholder needs are handled before being processed in system, software, or project requirement processes. It has a strong focus on identifying and analyzing initial stakeholder wishes and evolving requirements. Based on this it is especially useful in cases with high innovation or agile working models.

Stakeholder needs may span over multiple levels of abstraction (system, subsystem, software, hardware, organizational). Subsequently, there might not be a traceability for all given requirements towards the requirements in the context of System Requirements Analysis and Design (SYRD). Nevertheless, they are expected to be agreed and verified independently of their tracing path. It is important to note that stakeholder inputs refer not only to customer documents, but also standards, norms, regulatory and government requirements, as well as all relevant project partners.

In practical application, requirements elicitation involves all partners of the project independently of whether they are up- or downstream, external, or internal. This leads to a large number of people with whom to interact. Although communication is not rated within Automotive SPICE® Potential Analysis, stakeholder identification is an important indicator of whether the process purpose is fulfilled effectively. The complexity of the project is highly dependent on the number of stakeholders, and the project team shall be aware of that.

Evaluation of the stakeholder requirements supports the common understanding of stakeholder requirements. Within Automotive SPICE® Potential Analysis, this could also be implicitly demonstrated through the resulting system or software requirements in the System Requirements Analysis and Design (SYRD) and Software Requirements, Design and Implementation (SWDI) processes. Yet most importantly the agreement shall be reached after the evaluation to make sure all partners understand the requirement in the same way.

Changes in requirements may arise from different sources such as for instance changing technology, stakeholder needs, or legal constraints.

The Technical Change Request Management (TCRM) process is focused on agreed changes while Requirements Elicitation (REEL) is focused on reaching an agreement on evolving stakeholder needs. In practical applications these steps could be highly integrated, which shall be considered in the analysis.

5.8 SYRD System Requirements and Design

The purpose is to have a structured and analyzed set of system requirements and a system architectural design available.

5.8.1 General Information

As part of the System Level plugin, the System Requirements Analysis and Design (SYRD) process addresses the specification of the system based on requirement analysis and architectural design on the system level.

As the source of input to system development, stakeholder requirements often capture the needs from many different potentially conflicting or even contradictory perspectives. Analysis of stakeholder requirements and necessary trade-off are carried out to support the specification of a consistent set of requirements for the system. The system requirements (both functional and non-functional) are satisfied by the design solutions which are specified in the system architecture. Requirement analysis and architectural design need not be strictly sequential. System architectural design decisions may lead to iterative rework in system requirements, and vice versa.

5.8.1.1 Iterative vs. incremental development

Usually, the functional content in the product changes iteratively and evolves incrementally across releases. The term “increment” can be understood as adding a feature or element that did not exist before (analogy: building a house). The term “iteration” can be understood as refining, or adapting, an existing feature or element (analogy: a sculptor working on a sculpture).

Therefore, the complete set of requirements of the final product does not necessarily have to be available at the start of the project. Rather, release scopes agreed with the customer will define increments and iterative rework. In this respect, requirements creation can be driven by release definitions over time.

5.8.1.2 Structuring and prioritization of requirements

A possible and typical approach to prioritizing requirements is the allocation of requirements to releases. Since the scope of the Automotive SPICE® Potential Analysis may be different to the intended future project scope, prioritization is limited to the set of requirements related to the available project schedule. See *RAP.21 “Prioritization of requirements”*.

Further ways of structuring requirements may be realized by using attributes in tools for categorization, or a hierarchical headline structure with an adequate depth.

5.8.1.3 Specifying a system architecture

The system architectural design is the highest level of a design description of the system encompassing a collection of views dealing with different aspects (e.g., static structure, functional decomposition, dynamics) These views are architecture visualizations that are required for communication, discussion, reviews, analysis, evaluation, planning, change request analysis, impact analysis, maintenance etc. of the system.

There is no common definition of which views are required and no criteria for the completeness of such views. Essential views, however, are a static view providing an overview of the structure and a dynamic view describing the designated behavior behind system functionalities.

5.8.1.4 Special Characteristics

Since the Automotive SPICE® Potential Analysis only contains Requirements Elicitation plugin (REEL), System Level plugin (SYRD, SYIV) and Software Level plugin (SWDI, SWIV) as the three possible plugins (see Figure 3) and no provision yet for the other extensions (e.g., hardware

engineering HWE), the explicit derivation of Special Characteristics for non-software system elements in the system architecture as required in Automotive SPICE® PAM 4.0 is not covered by the Automotive SPICE® Potential Analysis.

5.8.2 Rating Rules within the process

5.8.2.1 Specification of system requirements

[SYRD.RL.1] If different approaches of documenting requirements are used concurrently (e.g., Word processor file, Application Lifecycle Management tool, database), the indicator BP1 shall not be downrated.

5.8.2.2 Analysis of system requirements

[SYRD.RL.2] If analysis results of requirements are not demonstrated by means of separate analysis reports or review records but by means of, e.g., tool-supported attributes or tool-supported commenting, the indicator BP1 shall not be downrated.

5.8.2.3 Structuring of system requirements

[SYRD.RL.3] If the notions “functional” and “non-functional” are not used as a structuring, categorization, or classification criterion, the indicator BP1 shall not be downrated.

5.8.2.4 Prioritization of system requirements

[SYRD.RL.4] If there is no evidence for prioritization but there is a separate release plan consistently mapping system functionality to future releases, the indicator BP1 shall not be downrated.

5.9 SYIV System Integration and Verification

The purpose is to integrate the system and to ensure that the integrated system is consistent with its provisions and compliant with the system requirements.

5.9.1 General Information

As part of the System Level plugin, the System Integration and Verification SYIV process addresses the integration of system elements and verification of the integrated system against the relevant requirements and architectural design specifications.

5.9.1.1 Specify verification measures for system integration and system verification

SYIV.BP1 and SYIV.BP2 require the identification of the necessary verification infrastructure and environment setup. This may be supported by using simulations of the environment such as hardware-in-the-loop simulations, vehicle network simulations, or digital mock-ups.

Verification results can support the update of simulation models.

5.9.1.2 Traceability and consistency

See chapter 4 for details on the consistency and traceability within the Automotive SPICE® Potential Analysis

5.9.2 Rating Rules within the process

5.9.2.1 Definition of verification measures

[SYIV.RL.1] If entry/exit criteria are reasonably specified for a set of verification measures instead of each individual verification measure, the indicators BP1 and BP2 shall not be downrated.

5.9.2.2 Automation of verification measures

[SYIV.RL.2] If a verification measure is automated and the correctness, completeness, and consistency of the corresponding scripts and programs are not addressed in the verification measure definition, the affected indicators BP1 or BP2 shall not be rated Green.

5.9.2.3 Exploratory testing

The testing state-of-the-art not only comprises testing derived from requirements, but also exploratory testing based on experience, such as “error guessing based on knowledge”. This is valuable as it adds to the quality of the product. Therefore, exploratory tests that are based on experience cannot be traced or demonstrated to be consistent with the system requirements by definition. Nevertheless, traceability is still needed between exploratory test cases and their results.

Notwithstanding the benefits, in principle exploratory testing alone cannot provide a reliable and conclusive evidence of verification of the system against the relevant specifications, which is often required from a standard, regulatory or customer perspective.

[SYIV.RL.3] If explorative tests used as verification measures do not have traceability to system requirements or system architecture, the indicator BP3 shall not be downrated.

5.10 MLEG Machine Learning Engineering

The purpose is to specify the requirements (for an ML model and corresponding ML data), and to provide a trained, validated, tested and deployed ML model.

5.10.1 General Information

For the development of Machine Learning elements MLEG is used as a consolidated process on the Machine Learning engineering activities. It focuses on whether the ML-related requirements, data basis, training, validation, testing, and verification are implemented, and evidenced in a traceable and risk-oriented manner. The objective is not to assess all detailed Machine Learning engineering activities separately, but to determine whether the essential prerequisites for a robust and verifiable ML result are sufficiently evident. Architecture-related aspects are not directly included as a separate topic; they are only considered indirectly through verification-related aspects such as verifiability, testability, and evidence generation.

5.10.1.1 Requirements and data basis:

MLEG considers whether the expected ML functionality, relevant functional and non-functional ML requirements, and the required ML data characteristics are appropriately defined and traceable. This includes checking whether the required data quality, data coverage, and origin of the data are understandable for the intended ML use case.

5.10.1.2 Training and validation:

MLEG also addresses whether the ML model is trained and validated in a controlled and reproducible way. This includes the use of defined training and validation data, a traceable training approach, and the consideration of typical ML risks such as overfitting, underfitting, or bias.

5.10.1.3 Testing and verification:

A central aspect of MLEG in the potential analysis is the evidence that the trained and deployed ML model fulfills the ML requirements. This requires an appropriate test approach, suitable test data, expected results, KPIs, pass/fail criteria, and meaningful test results. ML architecture aspects are not treated as a separate assessment topic in the potential analysis; they are only reflected indirectly where they influence verifiability, testability, training feasibility, or evidence generation.

5.10.2 Rating Rules within the process

Since the MLEG requirements belong to the group of software requirements the rating rules from SWDI “Software Requirements, Design and Implementation” should be considered here (see 5.5).

[MLEG.RL.1] If data characteristics or non-functional requirements of the ML data requirements are not addressed then MLEG.BP1 shall not be rated Green.

[MLEG.RL.2] If the ML training and validation approach uses validation techniques that do not require separated ML training and validation data sets at the start of ML training, then MLEG.BP2 shall not be downrated.

[MLEG.RL.3] If the ML test data set is used to perform major changes/optimization of the ML model, then MLEG.BP3 shall not be rated Green.

5.11 MLDM Machine Learning Data Management

The purpose is to define and align ML data with ML data requirements, maintain the integrity and quality of the ML data.

5.11.1 General Information

Machine Learning Data Management (MLDM) covers the establishment of an ML data management system, the development and application of data quality criteria, the processing of collected ML data, and the assurance of ML data quality. MLDM is a supporting process for Machine Learning Engineering (MLEG) and addresses the data dimension of ML development that is not covered by MLEG itself. Within the Automotive SPICE® Potential Analysis, MLDM is assessed to determine whether the ML data used in the exemplary project is managed in a traceable, controlled, and quality-assured manner.

The ML data requirements specified in MLEG serve as the primary input to MLDM. All MLDM activities — from data quality criteria to data processing and quality assurance — shall be traceable back to these requirements.

5.11.1.1 Establishing an ML data management system

An ML data management system shall support the complete ML data lifecycle, including the collection, labelling and annotation, structuring, versioning, and archiving of ML data. A status model for ML data sets shall be established to track the state of data throughout its lifecycle. The system shall be capable of supporting the quality criteria and activities defined in BP2.

5.11.1.2 Developing and applying quality criteria for ML data

Data quality criteria shall be defined based on the ML data requirements and shall address aspects such as relevant data sources, reliability and consistency of labelling, completeness against ML data requirements, and representativeness of the data for the intended ML use case. The defined quality criteria shall be documented and applied systematically throughout the data lifecycle.

5.11.1.3 Processing collected ML data

Collected raw data shall be processed — including annotation, analysis, and structuring — according to the ML data requirements. The relevant sources of raw data shall be identified and continuously monitored for changes, in particular for changes to the ODD that may affect the completeness or representativeness of the existing data sets. Where such changes are identified, the impact on the ML requirements and data requirements shall be assessed and, if necessary, fed back into MLEG.

5.11.1.4 Assuring quality of ML data

ML data quality assurance shall be performed according to the defined ML data quality approach. Suitable methods — such as sample-based reviews or statistical analysis — shall be applied to verify that the ML data meets the defined quality criteria. Evidence of these quality assurance activities shall be available and traceable to the quality criteria defined in MLDM.BP2.

5.11.2 Rating Rules within the process

5.11.2.1 Data quality criteria

[MLDM.RL.1] If the ML data management system does not support the data quality criteria and activities defined in BP2, the indicator BP1 shall not be rated Green.

5.12 PCOM Partner and Collaboration Management

The purpose is to select partners and collaborations according to relevant criteria and to monitor their performance against agreed commitments.

The usage and selection of the Partner and Collaboration Management (PCOM) process require some precaution for assessors.

The opportunity to include PCOM depends on the evaluated organization actually working with a partner or having a collaboration in the exemplary project.

The Partner and Collaboration Management (PCOM) process shall not be selected for evaluation of services solely based on professional staffing, personnel leasing or consulting services. Integration of such resources within a project may be observable within Potential Project Management (POPM).

For the Automotive SPICE® Potential Analysis, it is required to include the evaluation of supplier selection as further project collaboration may require subcontracting for technical or formal compliance management, such as for safety or security aspects.

Partnerships and collaborations can be complex with different roles and duties at the same time for one partner. Collaboration models can be complex with partners performing different functions in parallel. References for collaborations can be found for example in [AGILE_COL]. The traditional customer-supplier relationship is one of these scenarios, as also expressed within *RAP.13 “Partner and Collaborations”*.

5.12.1 General Information

All partnerships and collaborations can deal with one or both of following:

- A **product**, for example a commercial off-the-shelf software or system.
- A development **service** required to adapt or change the product, or even to develop one from scratch.

Both characteristics need to be managed individually for their differences in quality, maintenance, liability, and further characteristics. An agreement on partnerships and collaborations should respect these differences to enable systematic fulfillment and monitoring.

Agreements of partnerships and collaborations may need to follow dedicated documentation requirements, for example on cybersecurity development interface agreements or established requirements of specific industries.

Within Partner and Collaboration Management (PCOM) it should not be evaluated if an agreement represents consent of both parties, since the inspection of formal validity is not typically feasible for the assessor within the setup of an Automotive SPICE® Potential Analysis. Work products of PCOM may be sensitive for their information, as outlined by *RAP.14 “quotation and contracts”*.

5.12.1.1 Dictated collaborations and partnerships

Some collaborations and partnerships are not chosen but dictated by a customer or other collaboration partner. For such cases it is still required to identify deviations according to own policies, criteria and established agreements. Respective deviations need to be aligned with stakeholders, if applicable.

5.12.2 Rating Rules within the process

5.12.2.1 Internal organizations and affiliates

With reference to *RAP.11 “Delivery”*, Partner and Collaboration Management (PCOM) may also be evaluated for collaborations with internal organizations and company affiliates. The selection process

in this case may differ from an independent market selection due to needs for amortization of strategic investment, mergers and acquisitions. In such cases the selection for collaboration with an internal organization or affiliate may indicate a violation of respective selection criteria. This possible conflict cannot be sufficiently evaluated within the Automotive SPICE® Potential Analysis and therefore shall not be negatively reflected in its rating.

[PCOM.RL.1]: If the selection of collaborations and partnerships has been made for an internal organization or an affiliate company, although selection criteria are indicating a different opportunity as more favorable, the indicator BP2 shall not be downrated.

5.13 TCRM Technical Change Request Management

The purpose is to ensure that the technical change requests are analyzed, tracked, and implemented.

5.13.1 General Information

Technical Change Request Management (TCRM) may use the same workflow approach as Technical Problem Resolution (TEPR) or an independent, fully separated one.

Technical changes address the intended product directly. They typically influence the requirement set and originate in changed or specified stakeholder needs.

The focus in Technical Change Request Management (TCRM) is only on technical changes. The technical solution to a problem may be managed by a technical change request.

5.13.2 Rating Rules within the process

5.13.2.1 Analysis and assessment of change requests

The expectations for an adequate analysis of change requests cover these aspects:

- The input from all relevant stakeholders (internal and external) is considered including technical aspects and potential side effects, for example degraded functionality or compatibility problems.
- Technical feasibility, risks, complexity, and impact regarding the potential changes are systematically evaluated and documented.
- Modification and if applicable, potential alternatives are documented.
- Acceptance Criteria for confirmation of implementation are established (e.g., selection of existing regression test case(s), newly developed test case, review of all modified work products).
- Compliance with agreed regulations and policies is possible.

The analysis of technical change requests should be capable of identifying affected work products.

[TCRM.RL.1] If the analysis omits to address potential side effects, the indicator BP1 shall not be rated Green.

5.13.2.2 Track technical change requests to closure

Any action of a Technical Change request is to be tracked to closure, which could be represented by multiple final states. Final closure may depend on feedback from the initiator of the change itself which should therefore be sought in early and objective evaluation, for example in system demos or inspection meetings.

5.14 CSGE Cybersecurity Goal Elicitation

The purpose is to derive cybersecurity goals and to ensure traceability between the cybersecurity risk assessment and the cybersecurity goals.

Systematic cybersecurity management requires identification and evaluation of potential risks, the cybersecurity threats. They can be identified before, during and after project development. Within the Automotive SPICE® Potential Analysis, the identification process part however is not to be considered, analogue to *RAP.3 “Risk identification”*. Instead, the evaluation of recorded cybersecurity threats should be inspected for the impact to the project and consequent decisions for necessary counter measures.

5.14.1 General Information

Within cybersecurity engineering, various methods exist for the evaluation and management of threats, such as Threat Analysis and Risk Assessment (TARA), numerical and systematical evaluations, etc.

5.14.1.1 Threat analysis and cybersecurity risk evaluation

Threat analysis may include criteria for risk identification, exploitation, and occurrence to estimate the feasibility of attacks relevant for the project. Attacks can be described as a set of steps, that may be interchangeable for different ordering sequences – the attack paths. The evaluation and assessment of those scenarios should provide the information to motivate a justified decision for prevention and protection of the cybersecurity sensitive content and material – the cybersecurity assets.

The threat analysis and the risk evaluation shall include different aspects and viewpoints. For example, the influence on stakeholders, the different phases of the project's life cycle, impact on safety, privacy, operational and financial terms. For example, a phase between development and operations or manufacturing (Dev-Ops) may include handling requirements and setups to process assets in production ramp up phase that may be considered for the risk evaluation already in an early development phase.

5.14.1.2 Risk treatment options

The fundamental risk treatment options for cybersecurity are avoidance, reduction, acceptance, or transfer of risks. These risk treatment options can be consecutive and overlapping, for example when multiple attack paths are treated individually through different phases of the project.

Cybersecurity claims are not subject to further risk treatment; they include residual risks. They may need to be reevaluated when conditions change, for example new vulnerabilities are identified. As the scope of the Automotive SPICE® Potential Analysis is restricted, such as continuous activities cannot be consistently evaluated over lifetime, the systematic monitoring of related changes is not in scope. See *RAP.17 “Monitoring risks of cybersecurity”*.

5.14.1.3 Cybersecurity goals

Cybersecurity goals are high level requirements and need to be derived and aligned for avoidance and reduction of cybersecurity risks. Wherever new decisions contradict established cybersecurity goals, they need to be discussed and decided in dialogue with respective stakeholders. The definition of cybersecurity goals is not limited to the development of a product and may include post-development phases, such as production and decommissioning. Consistency of cybersecurity goals and threat scenarios can be supported by traceability.

5.15 CSVV Cybersecurity Verification and Validation

The purpose is to specify and verify the cybersecurity requirements, and to validate the cybersecurity goals.

5.15.1 General Information

The evaluation of Cybersecurity Verification and Validation (CSVV) depends on the inclusion of either software or system level (see Figure 3), which is selected from the Automotive SPICE® Potential Analysis (SYRD, SYIV, SWDI, SWIV).

Cybersecurity goals as defined within Cybersecurity Goal Elicitation (CSGE) are high-level requirements addressing an associated threat scenario. To achieve a cybersecurity goal, a set of cybersecurity requirements is specified. Corresponding design and implementation are not evaluated in the Automotive SPICE® Potential Analysis. Instead, the verification of the implementation against these requirements and goals is in scope of the Cybersecurity Verification and Validation (CSVV) process, see *RAP.19 “Cybersecurity Risk treatment Implementation”*.

Validation activities need to be defined, including effective methods to detect vulnerabilities not identified by the TARA and thus not addressed by specific risk treatment actions. Activities may include exploratory test methods such as Penetration tests, Fuzz test, etc. on different levels within a V-model. Evaluation of vulnerabilities shall not be reflected within the Cybersecurity Verification and Validation (CSVV) according to the rationale *RAP.18 “Vulnerability Analysis”*.

5.15.1.1 Risk treatment verification

Cybersecurity requirements are particularly desired characteristics of a system or software. Their verification will be performed within different integration levels, such as software units, integrated software, or a completely integrated system.

Static vulnerability checks can be a good measure but give a very selective picture on the CS dependability of the product.

5.15.1.2 Cybersecurity validation

The Cybersecurity validation activities are not consistently documented within related Output Information Items characteristics. This is a consequence of the update of the Automotive SPICE® for Cybersecurity Rev.1 that is planned after the release of this volume for consistency with Automotive SPICE® 4.0. Validation activities may include tests, exploratory tests or inspections related to the cybersecurity goals identified within Cybersecurity Goal Elicitation (CSGE). The validation environment shall be documented for validation activities.

Validation activities may be subcontracted for an improved level of independence, knowledge or confidentiality and may be defined iteratively. Such subcontracted services should be evaluated within CSVV and shall neither be reflected to POPM or PCOM.

Annex A Conformity of the process assessment and reference model

Introduction:

The Automotive SPICE® Potential Analysis process assessment and process reference model meet the requirements for conformance defined in [ISO33004].

The process assessment model can be used in the performance of assessments that meet the requirements of [ISO33002] with the exclusion for:

class 1 Assessment [ISO/IEC 33002, 4.6.1.1]

class 2 Assessment [ISO/IEC 33002, 4.6.1.2]

This clause serves as the statement of conformance of the process assessment and process reference models to the requirements defined in [ISO33004].

| *[ISO/IEC 33004:2015, 5.5 and 6.4]*

Due to copyright reasons each requirement is only referred to by its number. The full text of the requirements can be drawn from [ISO33004].

Conformance to the requirements for process reference models:

Clause 5.3, "Requirements for process reference models"

The following information is provided in chapters 1 and 2 of this document:

- the declaration of the domain of this process reference model
- the description of the relationship between this process reference model and its intended context of use
- the description of the relationship between the processes defined within this process reference model

The descriptions of the processes within the scope of this process reference model meeting the requirements of ISO/IEC 33004:2015 clause 5.3 are provided in chapter 3 of this document.

| *[ISO/IEC 33004:2015, 5.3.1]*

The relevant communities of interest and their mode of use and the consensus achieved for this process reference model are documented in the copyright notice and the scope of this document.

| *[ISO/IEC 33004:2015, 5.3.2]*

The process descriptions are unique. The identification is provided by unique names and by the identifier of each process of this document within chapter 3.

| *[ISO/IEC 33004:2015, 5.3.3]*

Clause 5.4, "Process descriptions"

The requirements for process descriptions are met by the descriptions of Process purpose and Process outcomes in chapter 3 of this document.

| *[ISO/IEC 33004:2015, 5.4]*

Conformance to the requirements for process assessment models:

Clause 6.1, "Introduction"

The purpose of this process assessment model is to support assessment of process performance capability for development and innovation in the automotive domain using the process measurement framework defined in chapter 2.2 within the scope specified in chapter 1.1.

| [ISO/IEC 33004:2015, 6.1]

Clause 6.2, "Process assessment model scope"

The process scope of this process assessment model is defined in the process reference model included in chapter 2.1 of this document. The Automotive SPICE® Potential Analysis process reference model is satisfying the requirements of ISO/IEC 33004:2015, clause 5 as described in this Annex.

The process capability scope of this process assessment model is defined in the process measurement framework, which defines a process measurement framework for process capability satisfying the requirements of ISO/IEC 33003:2015.

| [ISO/IEC 33004:2015, 6.2]

Clause 6.3, "Requirements for process assessment models"

The Automotive SPICE® Potential Analysis process assessment model is related to process capability.

| [ISO/IEC 33004:2015, 6.3.1]

This process assessment model incorporates the process measurement framework, which satisfies the requirements of ISO/IEC 33003:2015.

| [ISO/IEC 33004:2015, 6.3.2]

This process assessment model is based on the Automotive SPICE® Potential Analysis Reference Model included in this document.

This process assessment model is based on the defined measurement framework.

| [ISO/IEC 33004:2015, 6.3.3]

The processes included in this process assessment model are identical to those specified in the Process Reference Model.

| [ISO/IEC 33004:2015, 6.3.4]

For all processes in this process assessment model all levels defined in the process measurement framework are addressed.

| [ISO/IEC 33004:2015, 6.3.5]

This process assessment model defines

- the selected process quality characteristic in chapter 3
- the selected process measurement framework in chapter 2
- the selected process reference model(s) in chapter 2
- the selected processes from the process reference model in chapter 2

of this document.

| [ISO/IEC 33004:2015, 6.3.5 a-d]

In the capability dimension, this process assessment model addresses the process attribute and Capability Level defined in the process measurement framework.

| [ISO/IEC 33004:2015, 6.3.5 e]

Clause 6.3.1, "Assessment indicators"

Note: Due to an error in numbering in the published version of ISO/IEC 33004:2015 the following reference numbers are redundant to those stated above. To refer to the correct clauses from ISO/IEC 33004, the text of clause heading is additionally specified for the following three requirements.

The Automotive SPICE® Potential Analysis process assessment model provides a two-dimensional view of process capability for the processes in the process reference model, through the inclusion of assessment indicators as defined in chapter 2.3.1. The assessment indicators used are:

- Base practices and Output Information Items

| [ISO/IEC 33004:2015, 6.3.1 a, "Assessment indicators"]

Clause 6.3.2, "Mapping process assessment models to process reference models"

The mapping of the assessment indicators to the purpose and process outcomes of the processes in the process reference model is included in the tables of each process in chapter 4.

The mapping of the assessment indicators to the process attributes in the process measurement framework including the process attribute achievement is included in chapter 2.

| [ISO/IEC 33004:2015, 6.3.2, "Mapping process assessment models"]

Clause 6.3.3, "Expression of assessment results"

The process attributes and the process attribute ratings in this process assessment model are identical to those defined in the measurement framework. As a consequence, results of assessments based upon this process assessment model are expressed directly as a set of process attribute ratings for each process within the scope of the assessment. No form of translation or conversion is required.

| [ISO/IEC 33004:2015, 6.3.3, "Expression of assessment results"]

Annex B Information items characteristics

The information items and characteristics in this Annex are listed for convenience and are replications of Automotive SPICE® 4.0 and Automotive SPICE® for Cybersecurity 1.0, deviating only for bugfixes and improved representation. The Automotive SPICE® Potential Analysis uses only a subset of those information item characteristics for its reduced scope in comparison to these two PAM and PRM. See chapter 2.4 and 2.5 on the definition and explanation on how to interpret information items and their characteristics.

Information items are defined using the scheme in Table B.1.

Information item identifier	An identifier number for the Information item which is used to reference the Information item.
Information item name	Provides an example of a typical name associated with the Information item characteristics. This name is provided as an identifier of the type of Information item the practice or process might produce. Organizations may call these Information items by different names. The name of the Information item in the organization is not significant. Similarly, organizations may have several equivalent Information items which contain the characteristics defined in one Information item type. The formats for the Information items can vary. It is up to the assessor and the organizational unit coordinator to map the actual Information items produced in their organization to the examples given here.
Information item characteristics	Provides examples of the potential characteristics associated with the Information item types. The assessor may look for these in the samples provided by the organizational unit.

Table B.1 — Structure of IIC tables

ID	Name	Characteristics
01-03	Software component	Software component in design and implementation-oriented processes: The software architecture decomposes the software into software components across appropriate hierarchical levels down to the lowest-level software components in a conceptual model. Software component in verification-oriented processes: The implementation of a SW component under verification is represented, e.g., as source code, object files, library file, executable, or executable model. Identifies: • The Software element in the software architecture above the software unit level, or an implementation of such a software element. Includes: • Design model element, or executable source code such as libraries, modules, services or scripts.
01-50	Integrated software	A functional executable software which has been integrated from multiple software components. Identifies: • All configured software elements Includes: • Application parameter Examples and references: • Simulator with stubbing • Object code
01-52	Configuration item list	List of configurable items under configuration control. Identifies:

ID	Name	Characteristics
		- Name of configuration item - Work products - Unique reference to the configuration item Includes: - Configuration item attributes and properties
01-53	Trained ML model	Resulting output Machine Learning (ML) model of the ML training process Identifies: - Set of weights optimized during the training Includes: - Software representing the ML architecture - Set of hyperparameters
02-01	Commitment agreement	Mutual arrangement between two or more parties regarding terms of a transaction or relationship. Identifies: - All involved parties - Purpose of the collaboration - Definitions - Confidentiality - Termination conditions Includes: - Timings and durations - Resources, for example people and equipment - Efforts - Facilities - Responsibilities
02-50	Interface agreement	Interface agreement should include definitions regarding Identifies: - customer and supplier stakeholders and contacts - tailoring agreements - customer/supplier responsibilities (e.g., roles, RASIC chart) for distributed activities, including required actions in development and post-development Includes: - share of information/work products in case of issues (e.g., vulnerabilities, findings, risks) - agreed customer/supplier milestones - duration of supplier's support and maintenance
03-51	Machine Learning data set	Selection of data for Machine Learning training and validation, or test of a Machine Learning model. Identifies: - Patterns - Relationships - Features Includes: - Annotations and labels - ML Training and Validation Data Set - ML Test Data Set
03-53	ML data	Data used for Machine Learning, attributed by metadata. Identifies: - Unique ID - Attributes - Data characteristics, for example audio recordings, sensor data, pictures and videos - Data created by an algorithm

ID	Name	Characteristics
		Includes: Data created by processing of other data, for example added noise, changed colors or merged pictures
04-04	Software architecture	High-level design and structure of a software. Identifies: - Overall software structure - Functional behavior of the software components - Nonfunctional characteristics - Settings for application parameters - Technical characteristics of interfaces, for example application programming interface (API) - Dynamic behavior within different states and operating modes, for example: start-up, shutdown, calibration - Timing definitions for example slices, cycle times - Priorities, for example of processes and threats - Events handling, for example interrupts with their priorities Includes: - Justifying rationale for the chosen architecture - Explanatory annotations, for example with natural language, for single elements, diagrams or models.
04-05	Software detailed design	Internal structure and behavior of software elements. Identifies: - Control flows - Format of input/output data - Algorithms - Data structures - Variables Includes: - Justifying rationale for the chosen design - Interfaces - Explanatory annotations - Elements of semi-formal language, for example UML, SysML Examples and references: - Expression in formal or semi-formal language may be used in model based developed design
04-06	System architecture	High level design and structure of a system. Identifies: - Overview of the system structure - System elements - Behavior of system elements, for example operation modes, calibration sequences, performance. - Behavior with the environment - Interfaces between system elements and environment - Hardware-software interfaces, for example input-output pins of microcontrollers - Parameters, for example of resource and performance characteristics - Domain specific engineering references, for example mechanical engineering evaluations for thermal influence. Includes: - Justifying rationale for the chosen architecture - References to underlying architecture, for example Hardware architecture (04-52), Software architecture (04-06), or an ML-architecture (04-51) Examples and references:

ID	Name	Characteristics
		Vehicles wiring overview with identification of wiring technologies, control units and wireless interfaces for connectivity.
08-55	Risk treatment	Quantitative or qualitative value to express the level of a risk. Identifies: - Risk to be mitigated, avoided, or shared (transferred) - Related activities - Criteria for success or failure of activities - Frequency of monitoring Includes: - Exposure and detectability information - Originator - Alternative treatment options - Risk justifications, for example as claims Examples and References: - For CS [ISO/SAE 21434:2021, RQ-15-17]: avoiding, reducing, sharing, retaining the risk
08-56	Schedule	A plan that defines the times and sequences for events, tasks, or activities. Identifies: - Activities - Timing requirements, for example start and due dates - Dependencies between activities - Critical path Includes: - Progress evaluation, for example completion of individual activities - Scheduled resources - Input data - Evaluation of resource workload - Shared resources
08-58	Verification Measure Selection Set	A set of verification measures selected for a specific purpose. Identifies: - Verification measures - Scope of their application, for example a product variant, regression or a subcomponent Includes: - Identification of the verification measures - Criteria for re-verification, for example in the case of changes - Dependencies
08-59	Validation Measure	Tool or method used to ensure the accuracy and reliability of a measurement or test under realistic conditions to validate the intended use. Identifies: - Description of test scope - Measurement to be performed during the test - Test steps description - Pass/fail criteria, for example from end user survey Includes: - Simulation scenarios - Emulation - Entry criteria - Techniques and resources - Validation environment setup and configuration - Sequences

ID	Name	Characteristics
08-60	Verification Measure	Tool or method used to ensure the accuracy and reliability of a measurement or test under specified conditions to verify specified functionality. Identifies: • Description of test scope, for example fault injection safety case • Classifications, for example black-box or grey-box test • Measurement to be performed during the test, for example an optical inspection • Test steps description • Pass/fail criteria, for example from end user survey Includes: • Simulation scenarios • Emulation • Entry criteria • Equivalence classes and boundary values • Calculations and mathematical functions • Techniques and resources, for example review verification • Verification environment setup and configuration • Sequences
11-04	Product package release	Set of Elements delivered in the product release. Identifies: • Physical components • Elements necessary for intended use • Warnings and alerts • Application Parameters Includes: • Documentation to maintain or service the product • Information for the user, for example installation and setup instruction within a manual.
11-05	Software Unit	Software element not decomposed to a lower level. Identifies: • Single functions • Set of functions Includes: • Intended use and defined functionality, for example within a specification or an agreement Examples and References: • Representation of a software element at the lowest level in a conceptual model
11-06	Integrated System	Set of elements composed from different units or integrated sub-systems. Identifies: • The intended use • Boundaries, for example application parameters Includes: • All configured elements, for example references to requirements specification
11-50	Deployed ML model	Deployed ML model Identifies: • The source code derived from the trained ML model that shall be executed in the target system. Examples and references:

ID	Name	Characteristics
		- It may differ from the trained ML model which often requires powerful hardware and uses interpretative languages. - The deployed ML model is usually written in programming languages like C/C++.
13-06	Delivery evidence	Evidence of items shipped or electronically delivered to customer. Identifies: - Receiver - Delivery address - Delivery date - Acknowledgment of receipt Includes: - Identification information
13-07	Problem	Description of an issue. Identifies: - Submitter - Version it was identified - Classification, for example criticality, urgency or relevance - Project phase in which problem is recorded - Owner - Status - Technical root cause - Potential effects on other systems - Expected closure date Includes: - Identification - References to other affected domains, subprojects, or programs - Relationships to dependencies like changes, preventive measures or other problems
13-08	Baseline	A coherent set of work products which are consistent and complete and may serve as basis for next process steps and/or delivery. A baseline must be unique and not changed any more. Identifies: - All work products belonging to the baseline - References using the configuration item properties Includes: - Name - Version - State
13-14	Progress status	Set of indicators to document the achievements created by performing process activities according to the committed work to the former phase. Identifies: - Status of work activities, for example in respect to a plan - Evidence of the committed outcome - Fulfilment of criteria within the state model - Limitations of outcome or achievements in respect to the committed objectives, for example deviations of performed verification Includes: - Timing references, for example in relation to schedule, milestones - Efforts Examples and references: - Status of actual quality against planned quality
13-16	Change request	Request to change scope or impacts on planned activities or outcomes.

ID	Name	Characteristics
		Identifies: • Scope and purpose of the change activities • Originator of the change • Impacted operation environment • Process performance • Environment of usage for the process outcome • Infrastructure or resources • Documentation needs Includes: • Impacted outcomes and achievements • Process objectives • Approval for implementation of a change • Limitations to be considered • Criteria to verify the fulfillment of the implementation
13-19	Review evidence	A proof to demonstrate a structured check of a work product or a process has taken place. Identifies: • Name and version of the review object • Names and roles of the people who performed the review • Date • Status • Review criteria, for example review method, coverage, justification • Non-conformances found • Improvement suggestions Includes: • Documents considered, for example checklists, guidelines, work instructions • Time spent • Applicable standards
13-24	Validation results	Documented evidence confirming whether the end product meets the intended use expectations. Identifies: • Data, logs, feedback, or documentation • Measures passed • Measures not passed • Measures not executed • Rationale, for example security claims • Information about the execution (date, participants, etc.) • Abstraction or summary of results
13-50	ML test results	Results of ML test activities Identifies: • Test data and logs • Test data with correct results • Test data with incorrect results • Test data not executed, and a rationale Includes: • Information about the test execution (date, participants, model version etc.) • Abstraction or summary of ML test results
13-51	Consistency Evidence	Evidence of information to be semantically coherent along relevant artifacts, ensuring completeness, purpose and maturity of processes, tasks and products throughout their lifecycle. Identifies:

ID	Name	Characteristics
		- Traceability information, for example hyperlinks, repository location or editorial references. - Naming conventions - Relevant artifacts - Revision and revision history information - Change documentation and analysis information Includes: - Meta-information, for example database identifiers, notes in Git commits comments Examples and References: - Evidence of Definition of Done (DoD) adherence
14-01	Change history	Structured, chronological record of modifications made to an object (document, file, software component, etc.) over its lifecycle. Identifies: - Version information about changed object - Date of change - Description of change - Originator
14-02	Corrective action	Activity required to resolve a problem. Identifies: - Initial problem description - Ownership of activity - Definition of solution(s) - Series of actions Includes: - Timing needs, for example required closure or analysis date - Status indicator - Further activities needed, for example a follow up audit
14-10	Work package	Activities required to be performed in order to complete a set of work. Identifies: - Activities to be performed - Ownership, for example to a specific domain like verification. - Dependencies to other activities and work products - Input and output work products - Required information Includes: - Estimation of efforts and duration Examples and References: - Work package can be a statement of work document, for example to outsource activities to an engineering service.
14-50	Stakeholder groups list	A group of people, relevant to a specific purpose or domain. Identifies: - Persons and group of persons - Responsibilities of ownership - Representatives and roles Includes: - Information needs, for example reporting content and frequency. Examples and references: - Expert groups for specific domains, for example safety. - Executive board
15-06	Project status	Evaluated result for the relative state of a project Identifies: Progress and consistency to plans and schedule

ID	Name	Characteristics
		- Completed tasks - Relation to the intent of the project - Resources usage, for example hardware, material, human resources Includes: - Deviations and justification - Risks and opportunities to the planned progress and agreements - Issues and actions
15-08	Risk analysis	Summary of analyzed risks. Identifies: - Analyzed risks with their IDs - Impact scenarios (e.g., damage scenarios) Includes: - Potential ways to mitigate the risks - Selected risk treatment options (e.g., risk acceptance as cybersecurity claim or risk reduction) - Assumptions made - Probabilities of occurrence (e.g., attack feasibility) - Risk values - Constraints
15-09	Risk status	Status or change of an identified risk. Identifies: - Risk statement - Sources of the risk - Impact, for example in relation to severity and probability - Owner Includes: - Category - Threshold value(s) - Risk treatment activities and their progress
15-12	Problem status	Progress of problem resolution. Identifies - Containment and prevention activities - Dependencies status - References to status model Includes: - Problem categories and classification
15-21	Supplier evaluation	Results of the evaluation of one or more suppliers, based on the collected information and the check against the defined criteria. Identifies: - Context and scope information required (e.g., date of evaluation, parties involved) - Supplier selection criteria - Method and instrument (checklist, tool) used for evaluation - Requirements used for the evaluation - Assumptions and limitations Includes: - Purpose of evaluation - Fulfillment of evaluation requirements - Short list of the preferred suppliers
15-51	Analysis Results	Results of analysis of an object or task. Identifies: Object under analysis

ID	Name	Characteristics
		• Analysis criteria • Selection criteria or prioritization scheme • Decision criteria • Quality criteria Includes: • Decisions and selections performed • Assumptions and constraints • Evaluation criteria, for example correctness, completeness or consistency to a work product Examples and references: • Verifiability analysis results, for example when a test machine becomes defective • Results of a feasibility analysis
15-52	Verification Results	Results of verification activities. Identifies: • Identification information • Log data • Passed and failed results • Not executed/blocked verification activities • Test execution details, for example tester name, role. • Timing information Includes: • Summary of verification results • References, for example to problem resolution actions
15-55	Problem analysis evidence	Elements and documents proving a problem analysis is performed. Identifies: • Analyst and owner • Affected and involved parties • Context and root cause of the problem • Analysis results and summary • Potential impact, for example as severity or cost calculation Includes: • Date of the analysis • Potential solution(s)
16-03	Configuration management system	System to manage configurations throughout a project or product life cycle, providing integrity, consistency and control. Identifies: • Configuration items to be controlled, for example documents, hardware or tools • Configuration information, for example to a status model • Repository • Baselines • Changes and change status Includes: • Reporting requirements • Workflow of recovery and other containment activities, for example security fire drills. Examples and References: • NASA defines it as technical management discipline that provides visibility and control over performance, functional, and physical characteristics of a product, preventing incorrect or unsafe configurations from being released.
16-50	Organizational structure	Hierarchical overview and structure of a set of groups and persons interacting with each other for a specific activity. Identifies:

ID	Name	Characteristics
		• Hierarchical and functional reporting lines • Ownership and responsibilities • Organizational units Includes: • Interfaces • Locations • Communication details
16-52	ML data management system	Data management system supporting Machine Learning Engineering (MLEG). Identifies: • Data management activities • Data collection workflow • Labeling, Annotations and description • Ingestion • Exploration and profiling workflows • Procedure of structuring and cleansing • Related phases of engineering, for example ML training Includes: • References to configuration management • Information of data sources • Attributes to reference quality criteria for ML data Examples and References: • Supports the relevant sources of ML data
17-00	Requirement	Statement that identifies an operational, functional, or design characteristic, which is unambiguous, testable, measurable, and necessary for product or process acceptability. Identifies: • Expectation of functions and capabilities (e.g., non-functional requirements) • Owner and origin of the requirement • Identification information • Boundaries, for example target price range Includes: • Stakeholder viewpoint, for example black-box perspective • Design constraints, for example predefined and necessary implementation details. • Tolerances • Domain specific details, for example of safety and privacy standards Examples and references: • ISO/IEC directive quote: “expression, in the content of a document, that conveys objectively verifiable criteria to be fulfilled and from which no deviation is permitted if conformance with the document is to be claimed” • ISO/IEC 42010:2007 • Hardware level requirements for example mission profile, storage requirements of environment boundary definitions during environment test. • Operational expectations for example power consumption, crank behavior, heat dissipation boundaries. • Resource constraints, for example performance and memory space definition.
17-51	Cybersecurity goals	Describe a property of an asset that it is necessary to protect by means of

ID	Name	Characteristics
		cybersecurity Identifies: • Confidentiality needs • Authorization needs • Integrity needs • Availability needs Includes: • Goal Title • Objective • Scope • Key Metrics and success criteria • Milestones (if Applicable) • Action plan (if applicable) • Stakeholders involved • Link to potential risks • Budget and resources • Timeline • Compliance and standards • Sign-off and approval
17-53	Cybersecurity threat scenario	Description of how threats exploit a weakness/vulnerability or multiple weaknesses/vulnerabilities exposing assets to harm, to enable the corresponding risk analysis Identifies: • damage scenarios • Impact category • Sequence of actions that involve interaction with system resulting in a threat scenario • applicable threats, like ransomware, phishing, spoofing, denial of service Includes: • Detailed chronological and functional description of an actual or hypothetical threat or group of threats • asset targeted by the threat • cybersecurity property which is compromised • compromise cause of the cybersecurity property • Attack feasibility (high/medium/low/very low)
17-54	Requirement attribute	Information supporting structuring requirements for specific context or intent. Identifies: • Context and intent of requirement Includes: • Meta-attributes • Solution intent
18-07	Quality criteria	Specified requirements to determine whether a product, process, or service conforms to quality objectives. Identifies: • Measurement needs • Timings • Required elements • Needs for completeness • Accuracy • Performance needs Includes: • Thresholds • Tolerance level • Attributes

ID	Name	Characteristics
		- Compliance and conformance references Examples and References: - Conformance requirements specifying a specific set of values to be within a defined range.
18-50	Supplier evaluation criteria	Expectations for capabilities to be fulfilled by suppliers Identifies: - Conformance requirements - Product requirements - Project requirements - Requirements for continuous operation Includes: - Functional and non-functional requirements - Cybersecurity capabilities of a supplier's organization Examples and References: - ISO 21434 certificate
18-52	Escalation path	A sequence of organizational levels or responsible roles to which an unresolved issue, deviation, or risk shall be communicated in order to decision-making. Identifies: - Trigger conditions - Stakeholders and roles - Escalation methods - Decision authority Includes: - Level specific conditions for an escalation. - Communication and documentation requirements Examples and References: - A task force group requested by a customer includes an escalation path
18-57	Change analysis criteria	Definition of criteria to be included in the analysis of a change Identifies: - Resource requirements - Timing needs, for example to a project schedule - Risks and opportunities
19-50	ML data quality approach	Approach describing criteria and activities to satisfy ML data quality goals. Identifies: - Quality criteria, for example relevant data sources. - Analysis activities of the data Includes: - Reliability and consistency of labeling - Completeness against ML data requirements Examples and References: Quality criteria to avoid data bias

Annex C Bibliography

- [VDA63] Verband der Automobilindustrie e.V. (VDA) Band 6 Teil 3, Prozessaudit — Potenzialanalyse, Produkt- und Produktionsprozessentwicklung, Produkt- und Produktionsprozessrealisierung, Serienproduktion. Qualitäts Management Center (QMC), Berlin 2023
- [ASPICE_CS] Verband der Automobilindustrie e.V. (VDA) Automotive SPICE® for Cybersecurity 1st edition — Qualitäts Management Center (QMC), Berlin 2021
- [VDA_SUSA] Verband der Automobilindustrie e.V. (VDA) Supplier Self-Assessment — http://vda-gmc.de/wp-content/uploads/2023/02/VDA_SuSA_English-1.xlsx, Berlin 2023
- [AS40] Verband der Automobilindustrie e.V. (VDA) Automotive SPICE® Process Reference Model, Process Assessment Model, Version 4.0 — Qualitäts Management Center (QMC), Berlin 2023
- [AS_GL20] Verband der Automobilindustrie e.V. (VDA) Automotive SPICE® Guidelines, 2nd revised edition — Qualitäts Management Center (QMC), Berlin 2023
- [ISO33001] ISO/IEC 33001:2015, Information technology — Process assessment — Concepts and terminology, 2015-03
- [ISO33002] ISO/IEC 33002:2015, Information technology — Process assessment — Requirements for performing process assessment, 2015-03
- [ISO33003] ISO/IEC 33003:2015 Information technology — Process assessment — Requirements for process measurement frameworks, 2015-03
- [AGILE_COL] Agile Collaboration, 1st edition — Qualitäts Management Center (QMC), Berlin 2021
- [ISO33004] ISO/IEC 33004:2019 Information technology — Process assessment – Requirements for process reference, process assessment and maturity models
- [ISO33020] ISO/IEC 33020:2019, Information technology — Process assessment — Process measurement framework for assessment of process capability, 2019-11
- [ISO21434] ISO/SAE 21434, Road vehicles, Cybersecurity engineering, 2021-08
- [ISO26262] ISO 2626:2018, Road vehicles – Functional safety, 2018-12
- [ISO/PAS8800] ISO/PAS 8800:2024, Road vehicles – Safety and artificial intelligence

