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

1st edition, June 2024

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

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

Terms and glossary

Automotive SPICE® Potential Analysis consists of a subset of Automotive SPICE® 4.0 and Automotive SPICE® for Cybersecurity Rev.1. 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 Analysis are only representative for a limited period. The duration of the acceptance period must be agreed between the partners.

Compared to an Automotive SPICE® 4.0 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 to an agreed capability level. In any case, identified weaknesses can serve as input to an improvement program to prepare for a full Automotive SPICE® 4.0 Assessment without another prior Potential Analysis. As such, the Automotive SPICE® 4.0 Assessment also intends to increase the acceptance and application of Automotive SPICE®.

Automotive SPICE® Potential Analysis is based on the contents of Automotive SPICE® 4.0 and Automotive SPICE® for Cybersecurity 1.0, 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® 4.0 Assessment results.

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

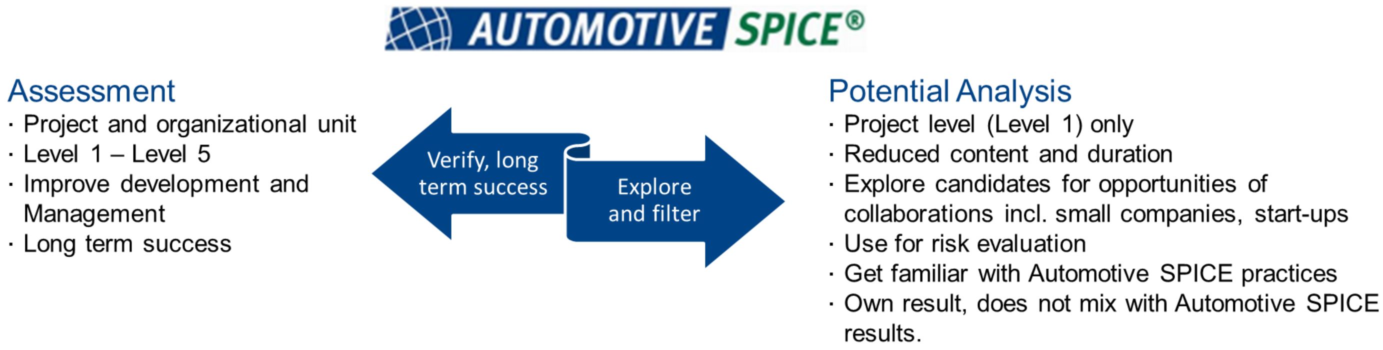
AUTOMOTIVE SPICE®
Assessment
· Project and organizational unit
· Level 1 – Level 5
· Improve development and Management
· Long term success
Verify, long term success
Explore and filter
Potential Analysis
· Project level (Level 1) only
· Reduced content and duration
· Explore candidates for opportunities of collaborations incl. small companies, start-ups
· Use for risk evaluation
· Get familiar with Automotive SPICE practices
· Own result, does not mix with Automotive SPICE results.

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 the 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 the 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 with 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.

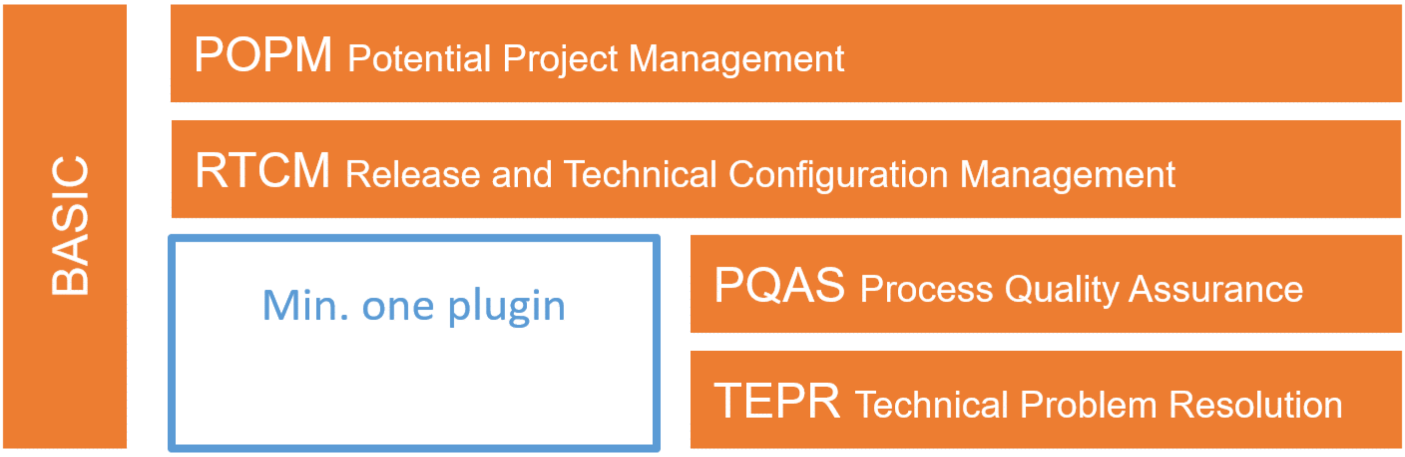
BASIC
POPM Potential Project Management
RTCM Release and Technical Configuration Management
Min. one plugin
PQAS Process Quality Assurance
TEPR Technical Problem Resolution

Figure 2 — Processes of the BASIC scope

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

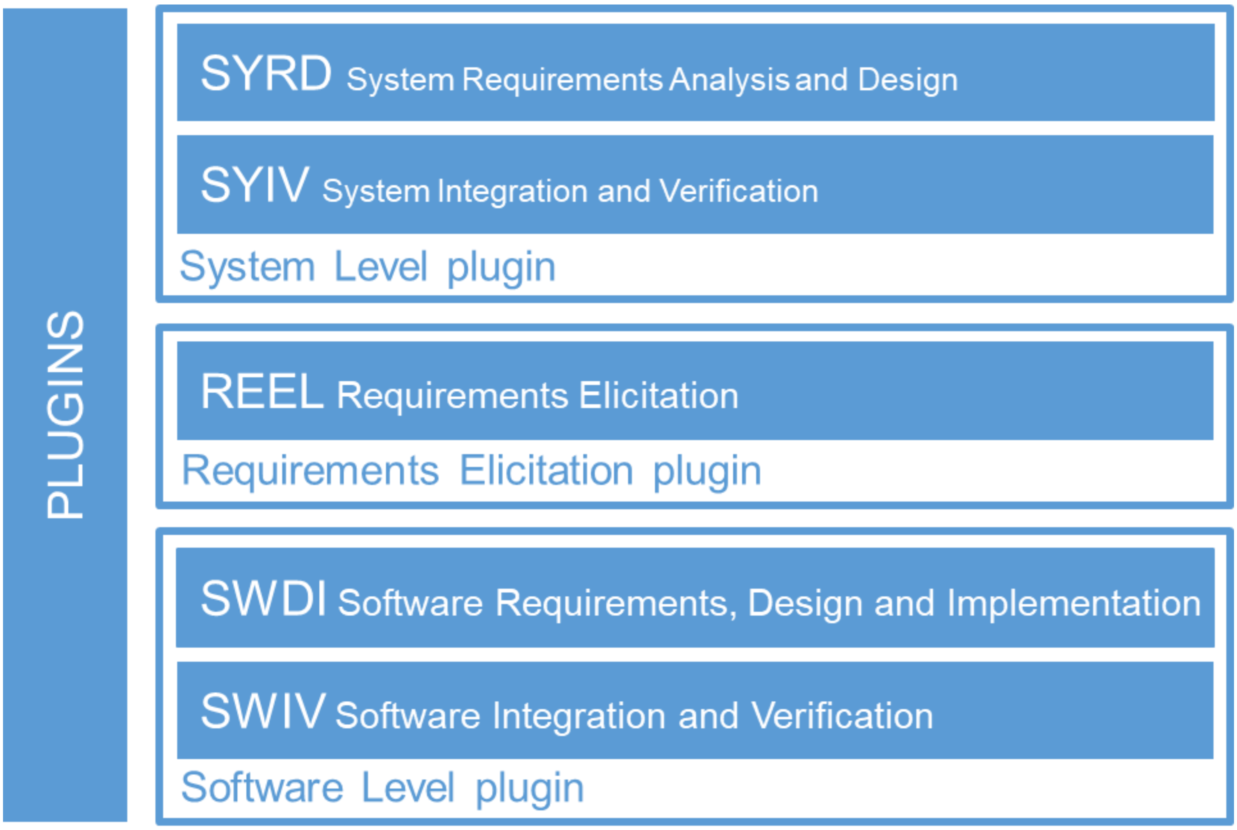
PLUGINS
SYRD System Requirements Analysis and Design
SYIV System Integration and Verification
System Level plugin
REEL Requirements Elicitation
Requirements Elicitation plugin
SWDI Software Requirements, Design and Implementation
SWIV Software Integration and Verification
Software Level plugin

Figure 3 — The three 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.

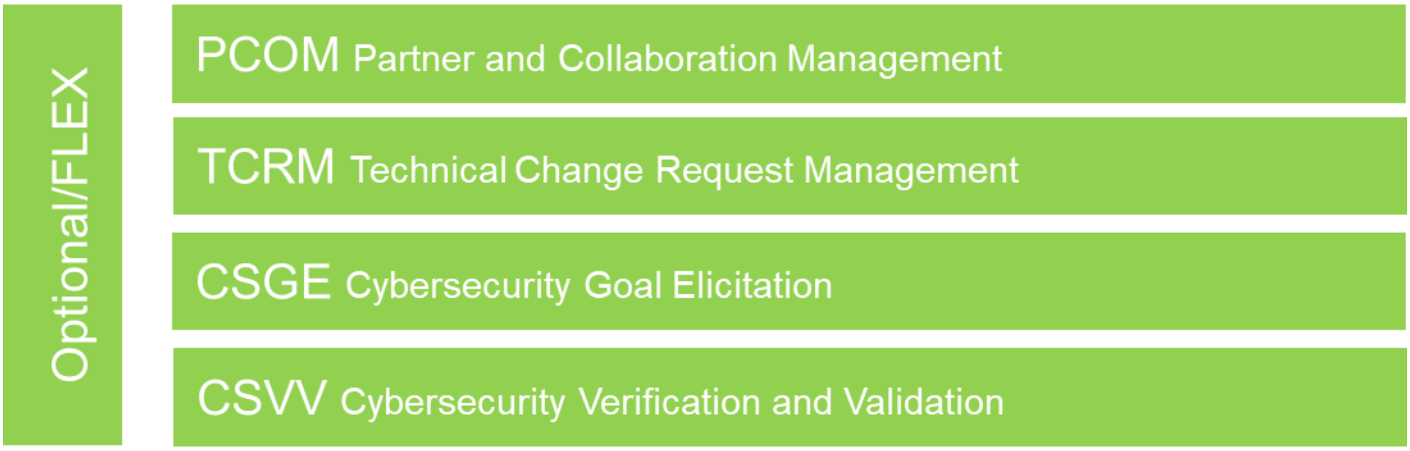
Optional/FLEX
PCOM Partner and Collaboration Management
TCRM Technical Change Request Management
CSGE Cybersecurity Goal Elicitation
CSVV Cybersecurity Verification and Validation

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 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 is the change 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 changes 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).

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. *Note: Refer to Annex B for the characteristics of each information item.*

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

The Automotive SPICE® Potential Analysis' highest level is process attribute *Process Performance* for process capability Level 1: Performed process.

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
The process performance process attribute is a measure of the extent to which the process purpose is achieved.
Process attribute achievements
As a result of full achievement of this process attribute: The process achieves its defined outcomes.

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 achieve 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. *Note: This includes documented and highlighted weaknesses that may become challenges for later phases of an intended collaboration and may require early improvement actions.*	*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 characterised 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.*
>
> *[ISO/IEC 33004:2015, 6.3.1]*

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 2.5 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).

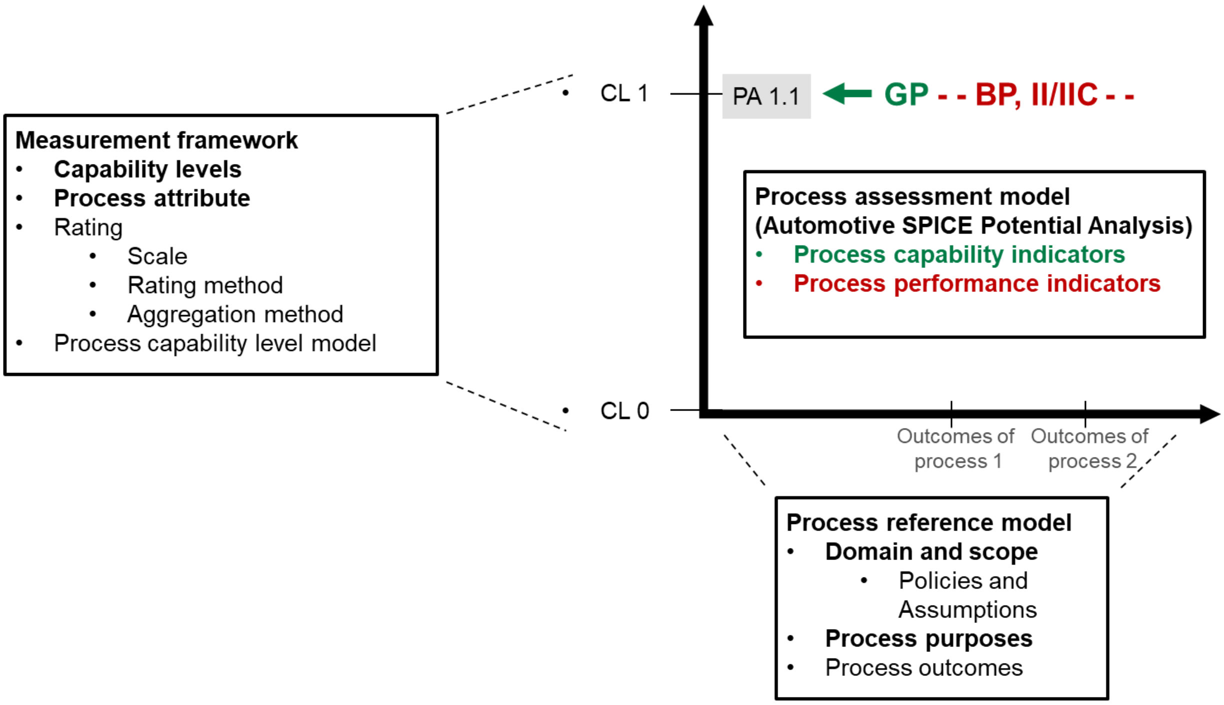

Figure 5 — Mapping model ASPICE PoA

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

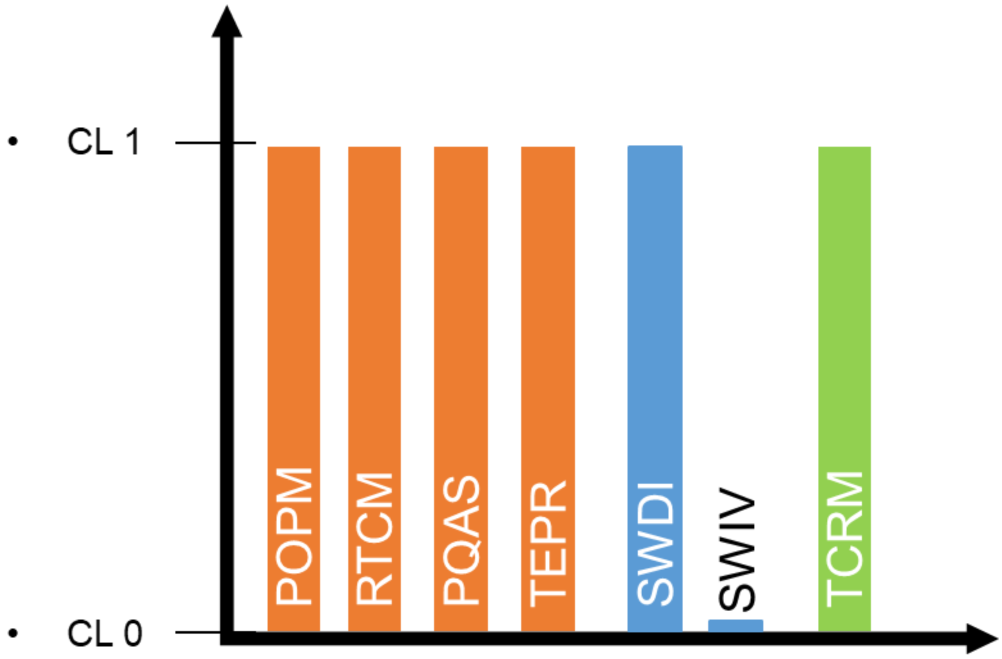

Figure 6 — Capability level per process (example)

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.

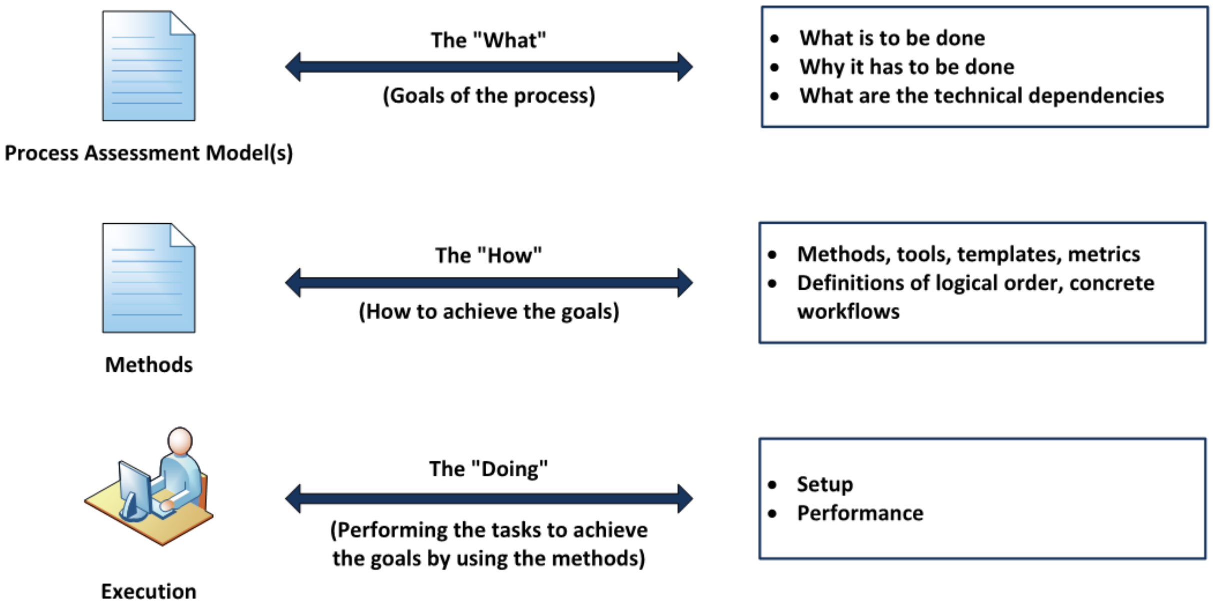
Process Assessment Model(s)
The "What"
(Goals of the process)
• What is to be done
• Why it has to be done
• What are the technical dependencies
Methods
The "How"
(How to achieve the goals)
• Methods, tools, templates, metrics
• Definitions of logical order, concrete workflows
Execution
The "Doing"
(Performing the tasks to achieve the goals by using the methods)
• Setup
• Performance

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.

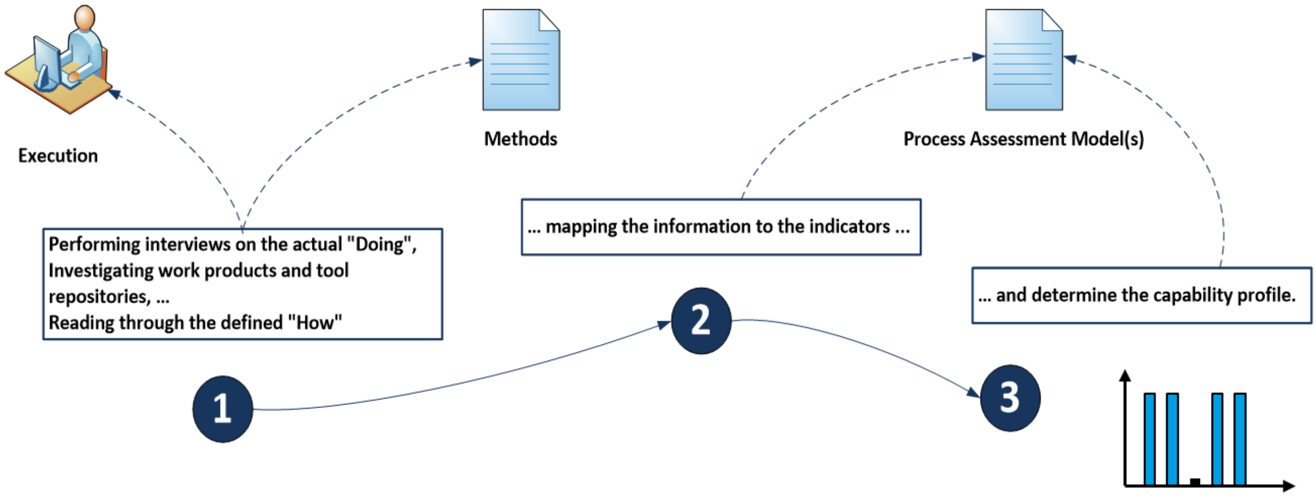
Execution
Methods
Process Assessment Model(s)
Performing interviews on the actual "Doing",
Investigating work products and tool
repositories, ...
Reading through the defined "How"
... mapping the information to the indicators ...
... and determine the capability profile.
1
2
3

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

Process outcomes

1) Activities are identified, sized, and estimated
2) Technical feasibility of the activities is evaluated
3) 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) Risks are managed continuously
7) Organizational problems related to the project are recorded, analyzed, and monitored

Base Practices

POPM.BP1: Identify, define, and estimate activities. Define estimates of effort for identified project activities and document 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 project interfaces. Identify and monitor interfaces of the project with internal or external stakeholders.

Note 1: Interfaces for partnerships and collaborations based on goods and work packages may be considered using Partner and Collaboration Management (PCOM).

POPM.BP4: Define and monitor project schedule. Schedule each activity of the project. Monitor the performance of 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.

Note 2: Progress for partnerships and collaborations based on goods and work packages may be considered individually using Partner and Collaboration Management (PCOM).

POPM.BP6: Manage risks. Manage risks to technical and organizational activities of the project. Ensure the impact of risk treatment activities is monitored for the project.

Note 3: Activities may be affected by technical, economical, and schedule related risks.

Note 4: Risk treatment options may include reduction, avoidance, transfer, or acceptance of risks.

POPM.BP7: Analyze and monitor organizational problems related to the project. Record, analyze and monitor the impact of 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 measure						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 activities	X						
BP2: Ensure technical feasibility	X	X					
BP3: Identify and monitor project interfaces			X				
BP4: Define and monitor project schedule				X			
BP5: Review progress of the activities			X	X	X		
BP6: Manage risks						X	
BP7: Analyze and monitor organizational problems 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) 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 affected parties
5) Baselines are regularly recorded and controlled for 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 engineering-related configuration items. Identify and document engineering-related configuration items.

RTCM.BP2: Control modifications and releases. Establish mechanisms to control the configuration items, and control modifications and releases using these mechanisms.

Note 1: Branch management may be used to manage complex software code.

RTCM.BP3: Establish baselines. Establish baselines for physical and logical integrity of the release, 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 engineering-related configuration items	X	X		X		X	
BP2: Control 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 processes comply with predefined provisions and that 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 process activities is verified, documented, and summarized
4) Non-conformances of process activities are recorded, analyzed, and managed until closure
5) Independent escalation mechanism is implemented

Base Practices

PQAS.BP1: Establish independency and objectivity for process quality assurance. Ensure process quality can be assured objectively without conflict of interests resulting from dependencies within organizational structures.

Note 1: Organizational structures may be influenced by hierarchy or standardized process frameworks.

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 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 resolution of non-conformances. 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 independency and objectivity for process quality assurance	X				
BP2: Implement an escalation mechanism					X
BP3: Define criteria to assure quality of process activities		X			
BP4: Ensure 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) Technical problems are recorded, analyzed, categorized, and assessed to identify an appropriate solution
2) Technical problem resolution is initiated
3) Technical problems are consistently tracked to closure
4) The status of problems and their trend are known

Base Practices

TEPR.BP1: Record technical problem, determine its cause and impact. Investigate the technical problem and determine its cause and impact to categorize the technical problem and to determine appropriate actions.

Note 1: Problem categorization may be based on severity, criticality (e.g., high, mid, low), or other criteria.

TEPR.BP2: Initiate technical problem resolution. Initiate appropriate actions to technically resolve the problem and include review of those actions.

TEPR.BP3: Track problems consistently to closure. Ensure the solution by tracking the status of problems to closure.

Note 2: The controlled resolution of problems may involve authorization of action(s), relationships, and dependencies (parent/child) and the adherence to schedule.

TEPR.BP4: Analyze problem trends. Collect and analyze 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 technical problem, determine its cause and impact	X			
BP2: Initiate technical problem resolution		X		
BP3: Track 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 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) Software units are developed according to the software detailed design

Base Practices

SWDI.BP1: Specify, analyze, structure and prioritize software requirements.
Specify, analyze and structure functional and non-functional software requirements according to defined characteristics for requirements. Prioritize software requirements according to project schedule.

Note 1: Software requirements can be structured, e.g., by categorizing, grouping, sorting, and prioritizing according to the project context.

SWDI.BP2: Specify and analyze 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 resource consumption objectives.

SWDI.BP3: Specify 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 software units. Develop and document 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 software requirements	X			
BP2: Specify and analyze software architectural design		X		
BP3: Specify software detailed design			X	
BP4: Develop 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 software units, integrate software and to ensure that the integrated software is consistent with its provisions and compliant with the software requirements.

Process outcomes

1) Verification measures for software units, for software component integration and for software verification are specified
2) Software units are verified with specified verification measures, and the verification results are recorded
3) Software components are integrated up to a complete integrated software, the integration is verified with specified verification measures, and the verification results are recorded
4) Integrated software is verified with 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 unit verification measures. Specify and perform software unit verification measures and record the verification results including pass/fail status.

Note 1: Examples for unit verification measures are static and dynamic analysis and code reviews.

SWIV.BP2 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 integration of the software elements until the software is fully integrated.

Note 2: Examples for preconditions for starting integration can be successful software element verification or qualification of pre-existing software elements

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.

Note 3: Horizontal traceability supports consistency, impact analysis and verification coverage demonstration for a respective V-model level.

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 unit verification measures	X	X			
BP2: Specify and perform the verification measures for 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 stakeholder needs and requirements of the exemplary product or service.

Process outcomes

1) Exchange of stakeholder expectations is established
2) Stakeholder requirements are agreed
3) Stakeholder needs are monitored continuously
4) Evolving stakeholder requirements are continuously evaluated

Base Practices

REEL.BP1: Obtain stakeholder expectations and requests. Obtain and define stakeholder expectations and requests through direct solicitation of stakeholder input and other sources containing inputs to stakeholder requirements, considering the target operating and hardware environment.

Note 1: Requirements elicitation may involve project partners up and downstream.

REEL.BP2: Agree on requirements. Formalize the stakeholder's expectations and requests into requirements. Reach a common understanding of the set of stakeholder requirements among affected parties by obtaining an explicit agreement from all affected parties.

Note 2: Reviewing the requirements and requests with the stakeholder supports a better understanding of stakeholder needs and expectations.

Note 3: The agreed stakeholder requirements may be influenced by feasibility studies, effort and schedule impact analysis.

REEL.BP3: Analyze changes on stakeholder requirements. Analyze all changes made to the agreed stakeholder requirements. Assess the impact and risks of the resulting modification.

Note 4: Accepted stakeholder change requests may be followed up by Technical Change Request Management (TCRM).

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 stakeholder expectations and requests	X			
BP2: Agree on requirements		X		
BP3: Analyze 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 system requirements.
Specify, analyze and structure functional and non-functional system requirements according to defined characteristics for requirements. Prioritize system requirements according to project schedule.

Note 1: System requirements can be structured, e.g., by categorizing, grouping, sorting, and prioritizing according to the project context.

Note 2: For changes to the stakeholder's requirements Technical Change Request Management (TCRM) may apply.

Note 3: The analysis of impact on effort and schedule supports the adjustment of project estimates. Refer to Potential Project Management (POPM).

SYRD.BP2: Specify and analyze 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: System requirements are analyzed, specified, structured, and prioritized	X	
BP2: System architectural design is analyzed and specified		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) Verification measures for system integration and for system verification are specified
2) System elements are integrated up to a complete integrated system, the integration is verified with specified verification measures, and the verification results are recorded
3) The integrated system is verified with 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 verification measures for integration. Specify and perform verification measures for the integration and record the verification results including pass/fail status. Perform integration of the system elements until the system is fully integrated.

Note 1: Examples for preconditions for starting integration can be successful system element verification or qualification of pre-existing system elements

SYIV.BP2: Specify and perform system verification measures for system. 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 system requirements and system architecture to the corresponding verification measures and results.

Note 2: Horizontal traceability supports consistency, impact analysis and verification coverage demonstration for a respective V-model level.

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 verification measures for integration	X	X		
BP2: Specify and perform system verification measures for system	X		X	
BP3: Establish horizontal traceability				X

3.10 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 performance against agreed commitments.

Process outcomes

1) Evaluation criteria for partners and collaborations are established
2) Partners and collaborations are evaluated against the defined criteria
3) Joint activities are agreed
4) Performance of the partners and collaborations is monitored against the agreements

Base Practices

PCOM.BP1: Establish evaluation criteria. Analyze relevant requirements to define evaluation criteria for capabilities of partners and collaborations.

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).

PCOM.BP2: Evaluate partners and collaborations against defined criteria. Collect information about the capabilities of partners and collaborations and evaluate it against the established evaluation criteria.

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.

PCOM.BP3: Agree on joint activities. Establish an agreement on joint activities, type and frequency of joint activities and reviews.

Note 3: Agreements may include ownership of processes, type and frequency of joint activities, failure management and reviews.

PCOM.BP4: Review performance of the partners and collaborations. Review 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 partners and collaborations against defined criteria		X		
BP3: Agree on joint activities			X	
BP4: Review performance of the partners and collaborations				X

3.11 TCRM Technical Change Request Management

Process ID

TCRM

Process name

Technical Change Request Management

Process purpose

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

Process outcomes

1) Technical change requests are analyzed, dependencies and relationships to other technical change requests are identified, and the impact is estimated
2) Implementation of technical change requests is confirmed
3) The status of all technical change requests is known, and technical change requests are tracked to closure

Base Practices

TCRM.BP1: Analyze and assess technical change requests. Technical change requests are analyzed by relevant parties according to analysis criteria. Work products affected by the change request and dependencies on other technical change requests are determined. The impact of the technical change requests is assessed.

NOTE 1: Examples for analysis criteria are: resource requirements, scheduling issues, risks, benefits, etc.

TCRM.BP2: Confirm the implementation of technical change requests. The implementation of technical change requests is confirmed before closure by relevant stakeholders.

TCRM.BP3: Track technical change requests to closure. The status of 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 technical change requests	X		
BP2: Confirm the implementation of technical change requests		X	
BP3: Track technical change requests to closure			X

3.12 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) Threats are analyzed and cybersecurity risks evaluated
2) Cybersecurity risk treatment options are determined
3) 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 threats and evaluate cybersecurity risks. Analyze threats to determine 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.

Note 1: Analysis may be for relevance to financial, safety, privacy, and operational terms.

CSGE.BP2: Define cybersecurity risk treatment option. For each cybersecurity risk define the selected treatment option to reduce, avoid, accept or transfer (share) the risks.

Note 2: Accepted and transferred (shared) risks can define cybersecurity claims that may require rationale and justification.

Note 3: Risks may be handled individually or as a set of risks.

CSGE.BP3: Derive and align cybersecurity goals for risk reduction and avoidance. Derive cybersecurity goals for 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.

Note 4: Traceability supports consistency and facilitates impact analyses.

Cybersecurity Goal Elicitation	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Output Information Items				
14-51 Cybersecurity scenario register	X			
15-08 Risk analysis	X	X		
08-55 Risk Measure		X	X	
13-20 Risk action request		X		
17-51 Cybersecurity goals			X	
13-51 Consistency Evidence				X
Base Practices				
BP1: Analyze threats and evaluate cybersecurity risks	X			
BP2: Define cybersecurity risk treatment option		X		
BP3: Derive and align cybersecurity goals for risk reduction and avoidance			X	
BP4: Establish traceability between the cybersecurity goals and the threat scenarios				X

3.13 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 cybersecurity goals 2) Risk treatment verification is specified and performed 3) Activities are identified and documented to validate cybersecurity goals and validation results are recorded 4) Traceability is established between the cybersecurity goals and validation results 5) Traceability is established between cybersecurity requirements and goals, and between the cybersecurity requirements and risk treatment verification specification

Base Practices
CSVV.BP1: Specify cybersecurity requirements for the cybersecurity goals. Specify functional cybersecurity requirements for the cybersecurity goals, including criteria for the achievement of the cybersecurity goals. *Note 1: This may include requirements for post-development phases such as preproduction, production, operation, maintenance, and decommissioning.*
CSVV.BP2: 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. *Note 2: Depending on the context the system might be a pure software system.*
CSVV.BP3: Cybersecurity validation activities are identified and documented. Cybersecurity validation activities are identified and documented to validate cybersecurity goals.
CSVV.BP4: Results of cybersecurity validation activities are recorded.
CSVV.BP5: Traceability is established. Ensure traceability between the cybersecurity requirements and goals and between the cybersecurity requirements and risk treatment verification specification. Ensure traceability between the cybersecurity goals and validation results. *Note 3: Traceability supports consistency, verification, and validation coverage demonstration.*

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
13-25 Verification result		X			
13-24 Validation Results				X	
08-59 Validation Measure			X		
Base Practices					
BP1: Specify cybersecurity requirements for the cybersecurity goals	X				
BP2: Cybersecurity verification measures are specified and performed		X			
BP3: Cybersecurity validation activities are identified and documented			X		
BP4: Results of 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 break down 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.

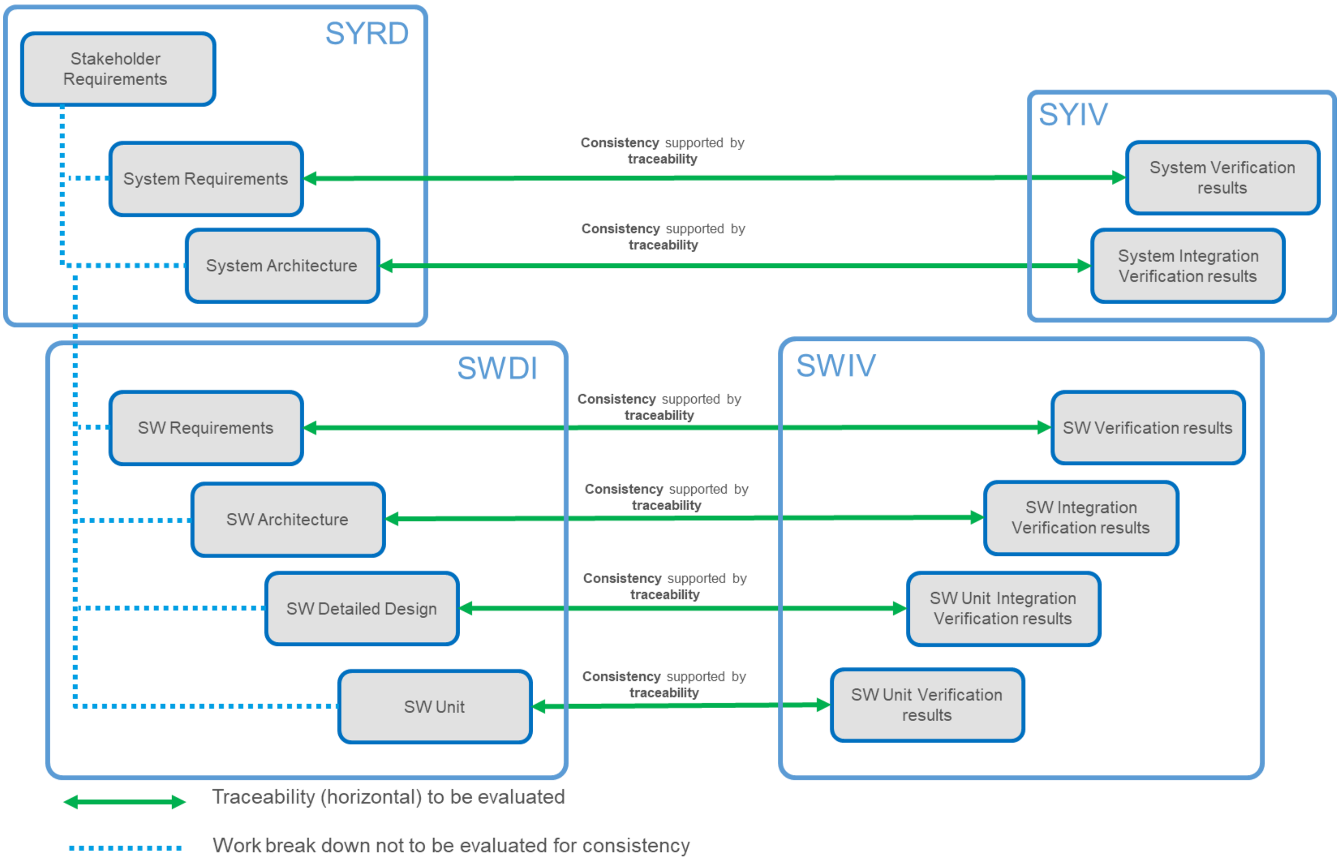
SYRD
Stakeholder Requirements
System Requirements
System Architecture
SYIV
System Verification results
System Integration Verification results
Consistency supported by traceability
Consistency supported by traceability
SWDI
SW Requirements
SW Architecture
SW Detailed Design
SW Unit
SWIV
SW Verification results
SW Integration Verification results
SW Unit Integration Verification results
SW Unit Verification results
Consistency supported by traceability
Consistency supported by traceability
Consistency supported by traceability
Consistency supported by traceability
Traceability (horizontal) to be evaluated
Work break down not to be evaluated for consistency

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 for the major elements, work products and information items. It shows the addon character of Cybersecurity Verification and Validation (CSVV), which requires the performance of at least System Level or Software Level plugin illustrated exemplary as V-model in Figure 10.

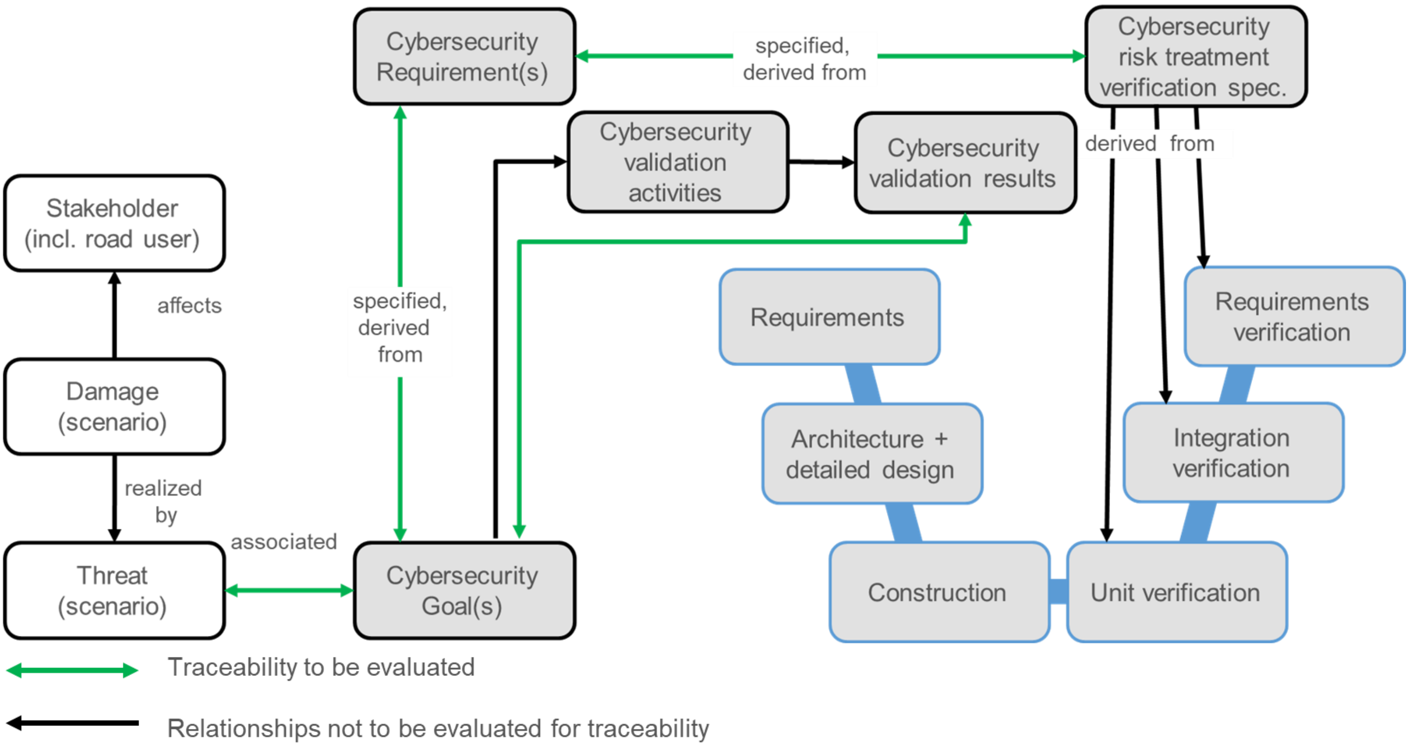
Cybersecurity Requirement(s)
specified, derived from
Cybersecurity risk treatment verification spec.
Cybersecurity validation activities
Cybersecurity validation results
derived from
Stakeholder (incl. road user)
affects
specified, derived from
Requirements
Requirements verification
Damage (scenario)
Architecture + detailed design
Integration verification
realized by
associated
Threat (scenario)
Cybersecurity Goal(s)
Construction
Unit verification
Traceability to be evaluated
Relationships not to be evaluated for traceability

Figure 10 — Consistency and relationships of Cybersecurity

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 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 chapter 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 n 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 element in the software architecture above the software unit level. • Represented by a design model element or executable code such as libs or scripts and a configuration description, if applicable.
01-50	Integrated software	• Software executable (e.g, simulator with stubbing, debug-able, object code) including: - application parameter files (being a technical implementation solution for configurability-oriented requirements) - all configured software elements
01-52	Configuration item list	• Items under configuration control • The name of work products and an associated reference (to file, to tool artifact) • Configuration item attributes and properties
02-01	Commitment agreement	• Signed off by all parties involved in the commitment/agreement • Establishes what the commitment is for • Establishes the resources required to fulfill the commitment, such as: - time - people - budget - equipment - facilities
02-50	Interface agreement	• Interface agreement should include definitions regarding - customer and supplier stakeholder and contacts

ID	Name	Characteristics
		- tailoring agreements - customer/supplier responsibilities (e.g., roles, RASIC chart) for distributive activities, including required actions in development and post-development - 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
04-04	Software architecture	• A justifying rationale for the chosen architecture. • Individual functional and non-functional behavior of the software component • Settings for application parameters (being a technical implementation solution for configurability-oriented requirements) • Technical characteristics of interfaces for relationships between software components such as: - Synchronization of Processes and tasks - Programming language call - APIs - Specifications of SW libraries - Method definitions in an object- oriented class definitions or UML/SysML interface classes - Callback functions, "hooks" • Dynamics of software components and software states such as: - Logical software operating modes (e.g, start-up, shutdown, normal mode, calibration, diagnosis, etc.) - intercommunication (processes, tasks, threads) and priority - time slices and cycle time - interrupts with their priorities - interactions between software components • Explanatory annotations, e.g, with natural language, for single elements or entire diagrams/models.
04-05	Software detailed design	• Elements of a software detailed design: - Control flow definition - Format of input/output data - Algorithms - Defined data structures - Justified global variables - Explanatory annotations, e.g, with natural language, for single elements or entire diagrams/models • Examples for expression languages, depending on the complexity or criticality of a software unit: - natural language or informal languages - semi-formal languages (e.g, UML, SysML) - formal languages (e.g, model-based approach)
04-06	System architecture	• A justifying rationale for the chosen architecture. • Individual behavior of system elements • Interrelationships between system elements - Settings for system parameters (such as application parameters) - Manual/human control actions, e.g., according to STPA • Interface Definitions:

ID	Name	Characteristics
		- Technical characteristics of interfaces for relationships between two system elements • Interfaces between system elements e.g.: - bus interfaces (CAN, MOST, LIN, Flexray etc.) - thermal influences - hardware-software-interfaces (HSI), see below - electromagnetic interfaces - optical interfaces - hardware-mechanical-interfaces (e.g., a cable satisfying both mechanical and electrical requirements, housing interface to a PCB) - hardware-mechanical interconnection technology such as connectors, pressfit - creepage and clearance distances • Fixations such as adhesive joints, screw bolts/fitting, riveted bolts, welding • System interfaces related to EE Hardware e.g.: - analogue or digital interfaces (PWM, I/O) and their pin configurations - SPI bus, I2C bus, electrical interconnections - placement, e.g., thermal interfaces between hardware elements (heat dissipation) - soldering - creepage and clearance distances • Interfaces for mechanical engineering e.g.: - friction - thermal influences - tolerances - clutches - fixations such as adhesive joints, screw bolts/fitting, riveted bolts, welding - forces (as a result of e.g., vibrations or friction) - placement - shape - A hardware-software interface, e.g.: - connector pin configurations and floating IOs for µCs/MOSFETs - signal scaling & resolution to be reflected by the application software • Mechanical-hardware interfaces e.g. - such as mechanical dimensioning - positioning of connectors - positioning of e.g., hall sensors in relation to the bus-bar - tolerances • Dynamics of system elements and system states: - Description of the system states and operation modes (startup, shutdown, sleep mode, diagnosis/calibration mode, production mode, degradation, emergency such as “limp-home”, etc.) - Description of the dependencies among the system components regarding the operation modes - Interactions between system elements such as inertia of mechanical components to be reflected by the ECU, signal propagation and processing time through the hardware and software and e.g., bus systems • Explanatory annotations, e.g., with natural language, for single elements or entire diagrams/models.

ID	Name	Characteristics
08-55	Risk measure	• Identifies - the risk to be mitigated, avoided, or shared (transferred) - the activities to mitigate, avoid, or share (transfer) the risk - the originator of the measure - criteria for successful implementation - criteria for cancellation of activities - frequency of monitoring • Risk treatment alternatives: - treatment option selected- avoid/reduce/transfer - alternative descriptions - recommended alternative(s) - justifications
08-56	Schedule	• Identifies the activities to be performed • Identifies the expected, and actual, start and completion date for required activities against progress/completion of activities • Identifies dependencies between activities and critical path • Has a mapping to scheduled resources and input data • Identifies resource allocation, resource workload, and critical resources • NOTE: A schedule is consistent with the defined work packages, see 14-10
08-58	Verification Measure Selection Set	• Include criteria for re-verification in the case of changes (regression). • Identification of verification measures, also for regression testing
08-59	Validation Measure	• A validation measure can be a test case, a measurement, a simulation, an emulation, or an end user survey • The specification of a validation measure includes - pass/fail criteria for validation measures (completion and end criteria) - a definition of entry and exit criteria for the validation measures, and abort and re-start criteria • Techniques • Necessary validation environment & infrastructure - Necessary sequence or ordering
08-60	Verification Measure	• A verification measure can be a test case, a measurement, a calculation, a simulation, a review, an optical inspection, or an analysis • The specification of a verification measure includes - pass/fail criteria for verification measures (test completion and ending criteria) - a definition of entry and exit criteria for the verification measures, and abort and re-start criteria • Techniques (e.g., black-box and/or white-box-testing, equivalence classes and boundary values, fault injection for Functional Safety, penetration testing for Cybersecurity, back-to- back testing for model-based development, ICT) • Necessary verification environment & infrastructure • Necessary sequence or ordering

ID	Name	Characteristics
11-04	Product release package	- Includes the hardware/software/product - Includes and associated release elements such as: - system hardware/software/product elements - associated customer documentation - application parameter definitions defined - command language defined - installation instructions - release letter
11-05	Software Unit	Can be - a representation of a software element at the lowest level in a conceptual model, which is decided not to be further subdivided and that is a part of a software component, or - a representation of a software unit under verification such as commented source code, auto-code, an object file, a library, an executable, or an executable model as input to verification
11-06	Integrated System	- Integrated product - Application parameter files (being a technical implementation solution for configurability-oriented requirements) - All configured elements for the product release are included
13-06	Delivery evidence	- Evidence of items shipped/delivered electronically to customer - Identification of: - to whom it was sent - address, where delivered - delivery date - receipt of delivered product
13-07	Problem	- Identifies the submitter of the problem - Identifies the group/person(s) responsible for providing problem resolution - Includes a description of the problem - Identifies classification of the problem (criticality, urgency, relevance etc.) - Identifies the status of the problem - States such as “open”, “in review”, “in implementation”, “closed”, “rejected”, “cancelled”, … - Transitions between states with conditions and authorities - Identifies the expected closure date
13-08	Baseline	- Identifies a state of one or a set of work products and artifacts which are consistent and complete - Basis for next process steps or delivery - Is unique and may not be changed *Note: This should be established before a release to identify consistent and complete delivery*

ID	Name	Characteristics
13-14	Progress status	• Status of a plan(s) (actual against planned) such as: - status of actual activities/work packages against planned activities/work package - status of actual results against established objectives/goals - status of actual resources allocation against planned resources - status of actual cost against budget estimates - status of actual time against planned schedule - status of actual quality against planned quality • Record of any deviations from planned activities and reason why
13-16	Change request	• Identifies purpose of change • Identifies requester contact information • Impacted system(s) • Impact to operations of existing system(s) defined • Impact to associated documentation defined • Criticality of the request, due date • Information supporting the tracking of change requests to closure - progress status attribute (e.g., open, allocated, implemented, closed) - time stamp of status change - person who changed a status • Rationale for changing a status
13-19	Review evidence	• Provides the context information about the review: - what was reviewed - lists reviewers who attended and their area of responsibility - status of the review • Provides information about the scope of the review: - checklists - review criteria - requirements - compliance to standards • Effort information about: - preparation time spent for the review - time spent in the review • Review findings: - non-conformances - improvement suggestions
13-20	Risk action request	• Date of initiation • Scope • Subject • Request originator • Risk management process context: - this section may be provided once, and then referenced in subsequent action requests if no changes have occurred - process scope - stakeholder perspective - risk categories - risk thresholds - project objectives - project assumptions - project constraints

ID	Name	Characteristics
		• Risks: - this section may cover one risk or many, as the user chooses - where all the information above applies to the whole set of risks, one action request may suffice - where the information varies, each request may cover the risk or risks that share common information - risk description(s) - risk probability - risk consequences - expected timing of risk • Risk treatment alternatives: - treatment option selected- avoid/reduce/transfer - alternative descriptions - recommended alternative(s) - justifications • Risk action request disposition: - each request should be annotated as to whether it is accepted, rejected, or modified, and the rationale provided for whichever decision is taken
13-24	Validation results	• Validation data, logs, feedback, or documentation • Validation measure passed • Validation measure not passed • Validation measure not executed, and a rationale • Information about the validation execution (date, participants etc.) • Abstraction or summary of validation results
13-25	Verification results	• Verification data and logs • Verification measure passed • Verification measure not passed • Verification measure not executed, and a rationale • Information about the verification execution (date, “object-under-verification”, etc.) • Abstraction or summary of verification results
13-51	Consistency Evidence	• Demonstrates bidirectional traceability between artifacts or information in artifacts, throughout all phases of the life cycle, by e.g., - tool links - hyperlinks - editorial references - naming conventions • Evidence that the content of the referenced or mapped information coheres semantically along the traceability chain, e.g., by - performing pair working or group work - performing by peers, e.g., spot checks - maintaining revision histories in documents - providing change commenting (via e.g., meta-information) of database or repository entries *Note: This evidence can be accompanied by e.g., Definition of Done (DoD) approaches.*

ID	Name	Characteristics
14-01	Change history	• Historical records of all changes made to an object (document, file, software component, etc.): - description of change - version information about changed object - date of change - change requester information - change control record information
14-02	Corrective action	• Identifies the initial problem • Identifies the ownership for completion of defined action • Defines a solution (series of actions to fix problem) • Identifies the open date and target closure date • Contains a status indicator • Indicates follow up audit actions
14-10	Work package	• Defines activities to be performed • Documents ownership for activities e.g., by domains • Documents critical dependencies to other work packages • Documents input and output work products • Documents the critical dependencies between defined work products • Information needed to perform these activities • Estimates of effort, duration *Note: The work package descriptions may be integrated into the/be a part of a schedule, see 08-56*
14-50	Stakeholder groups list	• Identifies: - involved parties - weight/importance of each stakeholder group - representative(s) for each stakeholder group - information needs of each stakeholder group
14-51	Cybersecurity scenario register	• Identifies: - damage scenarios - ID - title - description - impact category: - safety - financial - operational - privacy - quality • Threat scenarios - ID - asset concerned - security property: - confidentiality - integrity - availability - Attack feasibility (high/medium/low/very low)
15-06	Project status	• Status of in regards to progress and consistency of schedule, work item content, tasks, resources (human resources, infrastructure, hardware/materials, budget), skills and competence of human resources

ID	Name	Characteristics
		• planned progress and expenditure against dates/deadlines and actual expenditure • reasons for variance from planned progress • threats to continued progress • issues which may affect the ability of the project to achieve its goals • contingency actions
15-08	Risk analysis	• Identifies the risks analyzed • ID • Impact scenario (e.g., damage scenario) • Records the results of the analysis: - potential ways to mitigate the risk - selected risk treatment option (e.g., risk acceptance as cybersecurity claim or risk reduction) - assumptions made - probability of occurrence (e.g., attack feasibility) - risk value - constraints
15-09	Risk status	• Identifies the status, or the change, of an identified risk: - risk statement - risk source - risk impact and risk probability - categories and risk thresholds, e.g., for prioritization or setting a status • risk treatment activities in progress
15-12	Problem status	• Indicates progress of problem resolution • Status of problem e.g., - by problem categories/classification - by problem resolution stage
15-21	Supplier evaluation	• States the purpose of evaluation • Method and instrument (checklist, tool) used for evaluation • Requirements used for the evaluation • Assumptions and limitations • Identifies the context and scope information required (e.g., date of evaluation, parties involved) - Fulfillment of evaluation requirements
15-51	Analysis Results	• Identification of the object under analysis. • The analysis criteria used, e.g.: - selection criteria or prioritization scheme used - decision criteria - quality criteria • The analysis results, e.g.: - what was decided/selected - reason for the selection - assumptions made - potential negative impact • Aspects of the analysis may include - correctness - understandability - verifiability - feasibility

ID	Name	Characteristics
		- validity
15-52	Verification Results	• Verification data and logs • Verification measure passed • Verification measure not passed • Verification measure not executed • information about the test execution (date, tester name etc.) • Abstraction or summary of verification results
15-55	Problem analysis evidence	• Author and involved parties • Date of the analysis • Context and root cause of the problem • Analysis result may include - Impact - Potential negative impact - Affected parties • Potential solution (if known)
16-03	Configuration management system	• Supports the configuration management for the scope of the configuration item list contents • Correct configuration of products • Can recreate any release or test configuration • Ability to report configuration status - Has to cover all relevant tools
16-50	Organizational structure	• Disciplinary reporting line - Organizational units and sub-units, if applicable
17-00	Requirement	• An expectation of functions and capabilities (e.g., non-functional requirements), or one of its interfaces - from a black-box perspective - that is verifiable, does not imply a design or implementation decision, is unambiguous, and does not introduce contradictions to other requirements. - A requirements statement that implies, or represents, a design or implementation decision is called “Design Constraint”. • Examples for requirements aspects at the system level are thermal characteristics such as - heat dissipation - dimensions - weight - materials • Examples of aspects related to requirements about system interfaces are - connectors - cables - housing • Examples for requirements at the hardware level are - lifetime and mission profile, lifetime robustness - maximum price - storage and transportation requirements - functional behavior of analog or digital circuits and logic - quiescent current, voltage impulse responsiveness to crank, start-stop, drop-out, load dump - temperature, maximum hardware heat dissipation

ID	Name	Characteristics
		- power consumption depending on the operating state such as sleep-mode, start-up, reset conditions - frequencies, modulation, signal delays, filters, control loops - power-up and power-down sequences, accuracy and precision of signal acquisition or signal processing time - computing resources such as memory space and CPU clock tolerances - maximum abrasive wear and shearing forces for e.g., pins or soldering joints - requirements resulting from lessons learned - safety related requirements derived from the technical safety concept
17-51	Cybersecurity goals	• Describe a property of an asset, that is necessary to protect cybersecurity • Associated to one or more threat scenarios
17-54	Requirement Attribute	• Meta-attributes that support structuring and definition of release scopes of requirements. • Can be realized by means of tools. • NOTE: usage of requirements attributes may further support analysis of requirements.
18-07	Quality criteria	• Defines the expectations for work products and process performance • Including thresholds/tolerance levels, required measurements, required checkpoints • Defines what is an adequate work product (required elements, completeness expected, accuracy, etc.) • Defines what constitutes the completeness of the defined tasks • Defines what constitutes the performance of the defined tasks • Establishes expected performance attributes
18-50	Supplier evaluation criteria	• Expectations for conformity, to be fulfilled by competent suppliers • Links from the expectations to national/international/domains-specific standards/laws/regulations • Requirements conformity evidence to be provided by the potential suppliers or assessed by the acquiring organization • Provisions for tailoring or exception to the requirements
18-52	Escalation path	• Defined mechanisms to report and confirm escalation relevant issues • Identifies stakeholders to be included in the escalation path • Identifies levels of escalation
18-57	Change analysis criteria	• Defines analysis criteria, such as - resource requirements - scheduling issues - risks - benefits

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-qmc.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