VDA QMC

AUTOMOTIVE SPICE®

Automotive SPICE®

Process Reference and Assessment Model for Cybersecurity Engineering

Version 2.0

Title:	Automotive SPICE® for Cybersecurity Process Reference and Assessment Model
Author(s):	VDA Working Group 13
Version:	2.0
Date:	2025-03-28
Status:	Released

Copyright notice

Acknowledgement

The VDA, the VDA QMC and the Project Group 13 explicitly acknowledge the high-quality work carried out by the members of the intacs® working groups. We would like to thank all involved people who have contributed to the development and publication of Automotive SPICE®.

Derivative works

Document distribution

Change requests

Any problems or change requests should be reported through the defined mechanism at the www.vda-qmc.de web site.

Trademark notice

Document history

Version	Date	By	Notes
1.0	2021-07-16	VDA QMC PG13	First version
2.0	**2025-03-28**	**VDA QMC WG13**	**Revision of CS PAM, Adaption to 4.0**

Table of contents

List of Figures

List of Tables

1. Introduction

1.1. Scope

The UNECE regulation R155 requires, among others, that the vehicle manufacturer identify and manage cybersecurity risks in the supply chain. Automotive SPICE is a process assessment model which helps to identify process-related product risks when used with an appropriate assessment method. To incorporate cybersecurity-related processes into the proven scope of Automotive SPICE, additional processes have been defined in a Process Reference and Assessment Model for Cybersecurity Engineering (Cybersecurity PAM).

This document supplements the Automotive SPICE® 4.0 for enabling the evaluation of cybersecurity-relevant development processes.

A prerequisite for performing an assessment using the Automotive SPICE® for Cybersecurity PAM is the existence of an Automotive SPICE assessment result for the recommended VDA scope. Otherwise, an assessment using both the Automotive SPICE® for Cybersecurity PAM and Automotive SPICE® PAM for the recommended VDA scope processes has to be performed.

Annex B contains a subset of Information Item Characteristics that are relevant for the processes of Automotive SPICE® for Cybersecurity.

Annex C contains a subset of terms that are relevant for the processes of Automotive SPICE® for Cybersecurity.

1.2. Relation to ISO/SAE 21434

The purpose of an Automotive SPICE assessment is to identify systematic weaknesses in the primary processes, organizational processes and supporting processes.

An Automotive SPICE® for Cybersecurity assessment can identify gaps and process weaknesses in projects that are implementing cybersecurity activities. These gaps and weaknesses are a valuable input for improvements of the cybersecurity processes within the organization. By implementing effective improvement measures derived from assessment results the organization will be able to adjust and refine the cybersecurity management system.

Automotive SPICE® 4.0 and Automotive SPICE® for Cybersecurity cover system engineering, software engineering and hardware engineering. Indicators for mechanical engineering are not part of the current Automotive SPICE® PAMs.

By intention the risk scope of Automotive SPICE goes beyond the scope defined in ISO/SAE 21434. ISO/SAE 21434 focuses on the road user, whereas Automotive SPICE® for Cybersecurity addresses risks from the entire automotive eco-system that may have an impact on the development of cybersecurity relevant software-based systems.

Certain aspects of ISO/SAE 21434 are not in the scope of this document, as they are not performed in a development project context. They are addressed by ISO PAS 5112 and are subject to an audit of the cybersecurity management system.

The capability determination of processes for distributed cybersecurity activities, concept development, product development, cybersecurity validation, and threat analysis and risk assessment are supported by this document.

Project-dependent cybersecurity management is supported as follows:

- Cybersecurity responsibilities:
  GP 2.1.3: Determine resource needs.

- Cybersecurity planning:
  GP 2.1.2 – Plan the performance of the process and
  MAN.3 – Project Management.
- Tailoring of cybersecurity activities:
  PA 3.2 – Process deployment, and
  GP 2.1.2 – Plan the performance of the process.
- Reuse:
  included in make-buy reuse analysis SWE.2.BP3: Analyze software architecture,
  SYS.3.BP3: Analyze system architecture, and
  REU.2 – Management of Products for Reuse.
- Component out of context: covered by Cybersecurity Engineering Process Group (SEC) based on assumptions regarding cybersecurity goals.
- Off-the-shelf component:
  MAN.3.BP7 Define and monitor project interfaces and agreed commitments,
  Automotive SPICE® Guideline v2.0, chapter 2.5.3 Development external to the project, and
  MAN.7 – Cybersecurity Risk Management.
- Cybersecurity case:
  input provided by base practices “summarize and communicate results” of engineering processes.
- Cybersecurity assessment:
  Automotive SPICE® for Cybersecurity is a model for process capability determination. An in-depth technical analysis is not part of an Automotive SPICE® for Cybersecurity assessment.
- Release for post-development:
  SPL.2 – Product Release,
  SUP.8 – Configuration Management, and
  SUP.1 – Quality Assurance.
- Request for quotation:
  ACQ.2 Supplier Request and Selection
- Alignment of responsibilities:
  ACQ.4 Supplier Monitoring

1.3. Requirements on Assessment Scope

In general, the decision about the scope is at the discretion of the assessment sponsor.

When assessing the entire process profile using an existing assessment, the processes from SUP process group do not need to be re-evaluated. In cases where the assessment takes place in the context of a cybersecurity-relevant development, all cybersecurity-specific aspects in the PRM and PAM must be considered.

The validity of an existing assessment is generally described in chapter 10.2. in Automotive SPICE® Guidelines (2nd edition).

Rationale:

The Risk Treatment Validation process is focused on the cybersecurity goals where the validation process refers to all stakeholder goals or stakeholder requirements.

If the purposes of the respective processes are compared this becomes apparent.

The purpose of SEC.4 declares that it is to confirm that the integrated system achieves the associated cybersecurity goals.

However, the VAL.1 purpose is to provide evidence that the delivered product satisfies the intended use expectations in its operational target environment.

The cybersecurity goals are typically derived from the security properties under consideration of damage scenarios, and attack path analysis, including unintended use. This is either validated in the actual environment or a simulated environment.

Risk Treatment Validation is the proof that the unintended use should not lead to an undesired product behavior. The validation ensures that the expectation of the receiving party of the delivered product is fulfilled.

ACQ.2 is described as a process once performed in the sense of a potential analysis for a supplier, developing a cybersecurity relevant product. Therefore, it should be assessed in this certain context. The Automotive SPICE® for Potential Analysis on the other hand could be used in any case.

The scope of an Automotive SPICE® for Cybersecurity assessment may be tailored as appropriate. For example, if a supplier is not involved in the validation of cybersecurity goals, then SEC.4 may be excluded from the scope.

2. Statement of Compliance

The Automotive SPICE process assessment and process reference models conform with ISO/IEC 33004:2015 and can be used as the basis for conducting an assessment of process capability.

Automotive SPICE® 4.0 is used as an ISO/IEC 33003:2015-compliant measurement framework.

A statement of compliance of the process assessment and process reference models with the requirements of ISO/IEC 33004:2015 is provided in Annex A.

A statement of compliance of the measurement framework with the requirements of ISO/IEC 33003:2015 is provided in Annex A of Automotive SPICE® 4.0.

3. Process Capability Determination

The concept of process capability determination by using a process assessment model is based on a two-dimensional framework. The first dimension is provided by processes defined in a process reference model (process dimension). The second dimension consists of capability levels that are further subdivided into process attributes (capability dimension). The process attributes provide the measurable characteristics of process capability.

The process assessment model selects processes from a process reference model and supplements them with indicators. These indicators support the collection of objective evidence which enable an assessor to assign ratings for processes according to the capability dimension.

The relationship is shown in Figure 1:

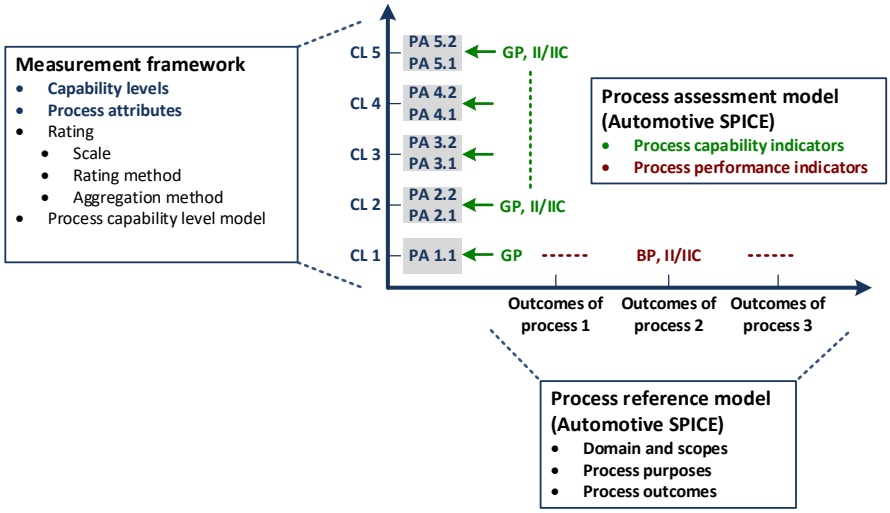

Figure 1 — Process Assessment Model Relationship

3.1. Process reference model

Processes are collected into process groups according to the domain of activities they address.

These process groups are organized into 3 process categories: Primary processes, Organizational processes and Supporting processes.

For each process a purpose statement is formulated that contains the unique functional objectives of the process when performed in a particular environment. For each purpose statement a list of specific outcomes is associated, as a list of expected positive results of the process performance.

For the process dimension, the Automotive SPICE® and Automotive SPICE® for Cybersecurity process reference models provide the set of processes shown in Figure 2. In this document the processes that are relevant for cybersecurity are described. For other processes see Automotive SPICE® 4.0.

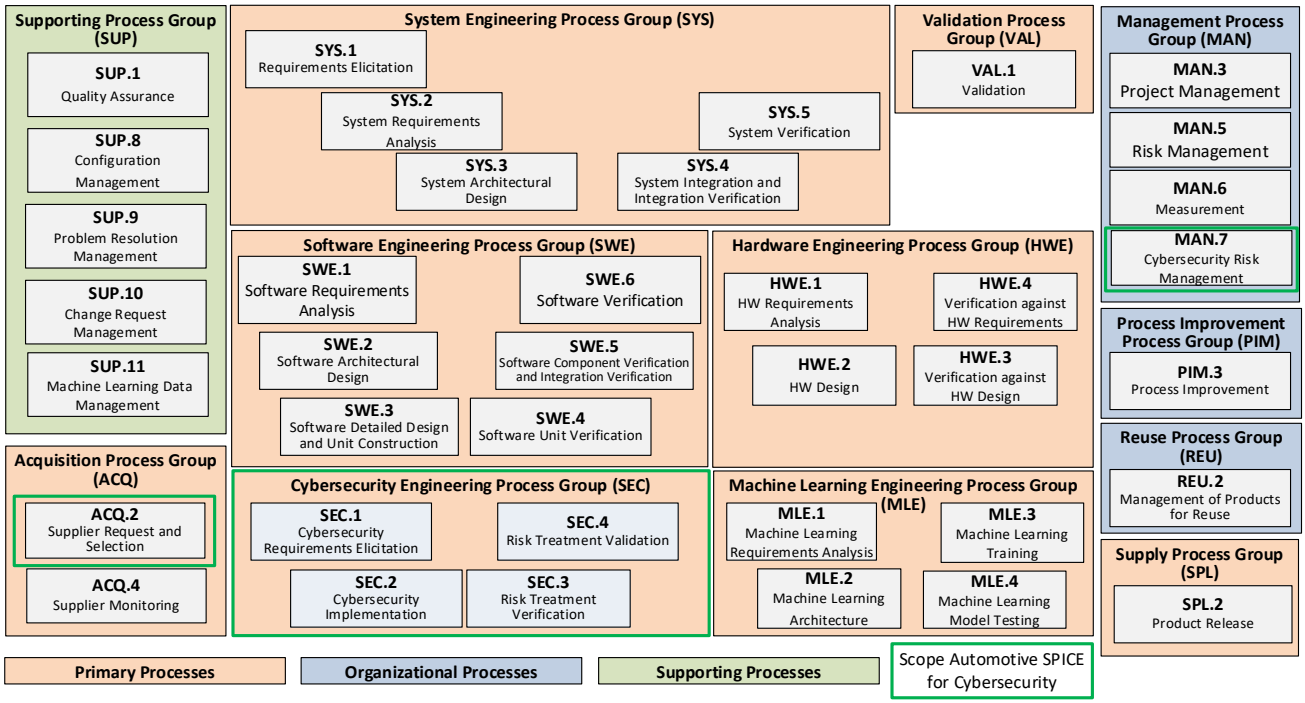

Figure 2 — Automotive SPICE® + Cybersecurity Process Reference Model – Overview

3.1.1. Primary Processes category

The primary processes category consists of processes that may apply for an acquirer of products from a supplier or may apply for product development when responding to stakeholder needs and delivering products including the engineering processes needed for specification, design, implementation, integration, and verification.

The primary processes category for Automotive SPICE® for Cybersecurity consists of the following process groups:

- the Acquisition Process Group
- the Cybersecurity Engineering Process Group

The Acquisition Process Group (ACQ) consists of processes that are performed by the customer, or the supplier when acting as a customer for its own suppliers, in order to acquire a product and/or service.

ACQ.2	Supplier Request and Selection

Table 1 — Primary Life Cycle Processes – ACQ

The Cybersecurity Engineering Process Group (SEC) consists of processes performed in order to achieve cybersecurity goals.

SEC.1	Cybersecurity Requirements Elicitation
SEC.2	Cybersecurity Implementation
SEC.3	Risk Treatment Verification
SEC.4	Risk Treatment Validation

Table 2 — Primary Processes – SEC

3.1.2. Organizational Processes category

The Organizational Processes category consists of processes that develop process, product and resource assets which, when used by projects in the organization, will help the organization achieve its business goals.

The Organizational Processes category for Automotive SPICE® for Cybersecurity consists of the following group:

- the Management Process Group

The Management Process Group (MAN) consists of processes that may be used by anyone who manages any type of project or process within the life cycle.

MAN.7	Cybersecurity Risk Management

Table 3 — Organizational Processes – MAN

3.2. Measurement framework

The process capability levels, process attributes, rating scale and capability level rating model are identical to those defined in Automotive SPICE® 4.0.

3.3. Understanding the level of abstraction of a PAM

The term "process" can be understood at three levels of abstraction. Note that these levels of abstraction are not meant to define a strict black-or-white split or provide a scientific classification schema. The message here is to understand that, in practice, when it comes to the term "process" there are different abstraction levels, and that a PAM resides at the highest.

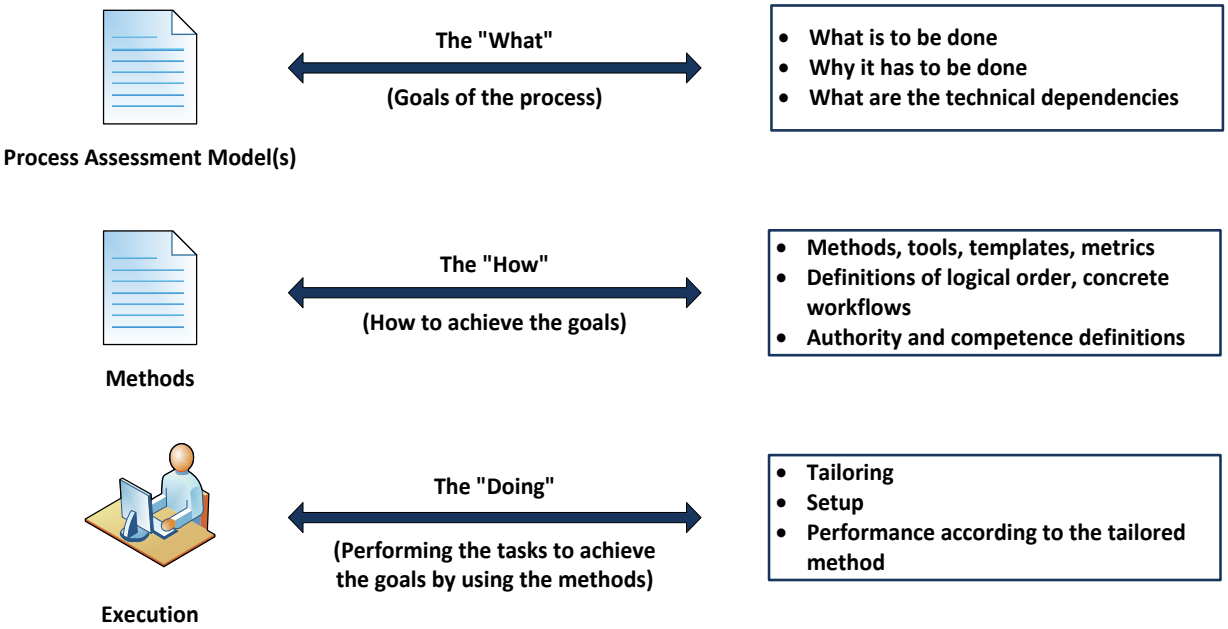

Figure 3 — Possible Levels of Abstraction for the Term "Process"

Capturing experience acquired during product development (i.e., at the DOING level) in order to share this experience with others means creating a HOW level. However, a HOW is always specific to a particular context such as a company, organizational unit or product line. For example, the HOW of a project, organizational unit, or company A is potentially not applicable as is to a project, organizational unit or company B. However, both might be expected to adhere the principles represented by PAM indicators for process outcomes and process attribute achievements. These indicators are at the WHAT level, while deciding on solutions for concrete templates, proceedings, tooling, etc. is left to the HOW level.

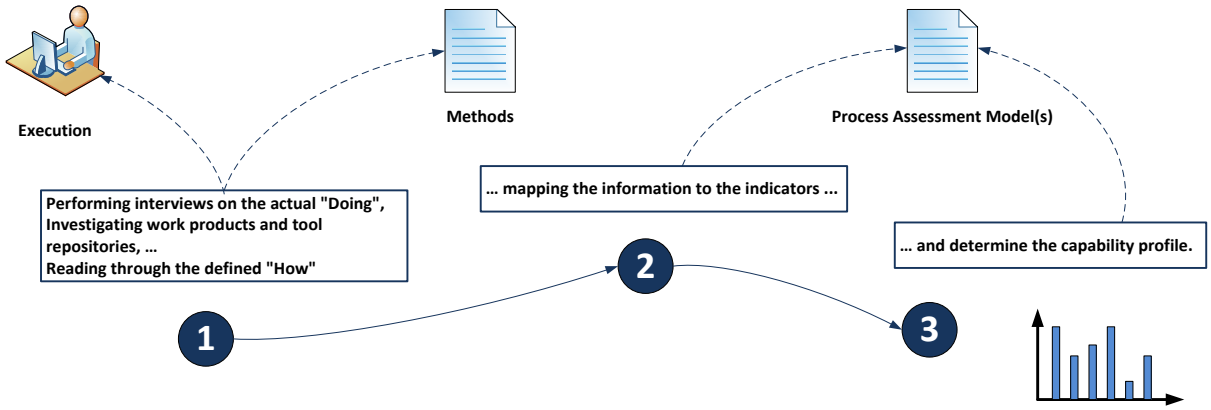

Figure 4 — Performing a Process Assessment for Determining Process Capability

4. Process Reference Model and Performance Indicators (Level 1)

4.1. Acquisition Process Group (ACQ)

4.1.1. ACQ.2 Supplier Request and Selection

Process ID
ACQ.2
Process name
Supplier Request and Selection
Process purpose
The purpose is to select a supplier for a commitment/agreement based on relevant criteria.
Process outcomes
1) Evaluation criteria are established for suppliers. 2) Suppliers are evaluated against the defined criteria. 3) A request for quotation is issued to supplier candidates. 4) Commitment/agreement, corrective actions, are agreed. The supplier is contracted in consideration of the evaluation result.

Base practices
ACQ.2.BP1: Establish supplier evaluation criteria. Analyze relevant requirements to define evaluation criteria for supplier's capabilities. *Note 1: The definition of evaluation criteria may consider:* • *Functional and non-functional requirements* • *Technical evaluation regarding cybersecurity capabilities of the supplier, including cybersecurity concepts and methods (threat analysis and risk assessment, attack models, vulnerability analysis, etc.)* • *The capability of the supplier's organization concerning cybersecurity (e.g., cybersecurity best practices from the development, applicable post-development activities (e.g. production, operation and decommissioning), governance, quality, and information security)* • *Continuous operation, including cybersecurity* • *Supplier capability and performance evidence in terms of cybersecurity obtained by supplier monitoring in the previous projects.*
ACQ.2.BP2: Evaluate potential suppliers. Collect information about the supplier's capabilities and evaluate it against the established evaluation criteria. Short-list the preferred suppliers and document the results. *Note 2: The evaluation of potential suppliers may be supported by:* • *Summaries of previous Automotive SPICE® for Cybersecurity assessments* • *Evidence of the organizational cybersecurity management system (e.g., organizational audit results if available)* • *Evidence of an information security management system* • *Evidence of the organization's quality management system appropriate/capable of supporting cybersecurity engineering* • *Experience from previous acquisitions*

ACQ.2.BP3: Prepare and issue a request for quotation. Identify supplier candidates based on the evaluation. Prepare and issue a request for quotation including a corrective action plan for identified deviations.

ACQ.2.BP4: Negotiate and award the commitment/agreement. Establish a commitment/agreement based on the evaluation of the request for quotation responses, covering the relevant requirements, and the agreed corrective actions.

Note 3: Distributed cybersecurity activities may be specified within a cybersecurity interface agreement considering all relevant aspects (e.g., contacts, tailoring, responsibilities, information sharing, milestones, timing).

Note 4: In case of deliverables without any support (e.g., free and open-source software), an interface agreement is not required.

ACQ.2 Supplier request and selection	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Output Information Items				
02-01 Commitment/agreement				X
02-50 Interface agreement				X
08-55 Risk treatment				X
12-01 Request for quotation			X	
14-02 Corrective action			X	X
15-21 Supplier evaluation		X		
18-50 Supplier evaluation criteria	X	X		
Base Practices				
BP1: Establish supplier evaluation criteria.	X			
BP2: Evaluate potential suppliers		X		
BP3: Prepare and issue a request for quotation			X	X
BP4: Negotiate and award the commitment/agreement				X

4.2. Management Process Group (MAN)

4.2.1. MAN.7 Cybersecurity Risk Management

Process ID
MAN.7
Process name
Cybersecurity Risk Management
Process purpose
The purpose is to regularly identify, analyze, prioritize, and monitor risks of damage to relevant stakeholders.
Process outcomes
1) The item is defined including its functions and boundaries. 2) Relevant assets, threats and damage scenarios are identified and regularly updated. 3) Cybersecurity risks are analyzed based on impact rating and attack feasibility rating in order to support prioritization for the treatment of risks. 4) The status of risk and the progress of the risk treatment activities is determined. 5) Appropriate treatment is taken to mitigate the impact of risk based on its priority, likelihood, and consequence or other defined risk threshold.

Base Practices
MAN.7.BP1: Identify cybersecurity risk management scope. Identify and regularly update the cybersecurity risk management scope including the item, its functions and its boundaries with affected parties. *Note 1: Risks may include technical, economical, and schedule risks.* *Note 2: Risks may include the suppliers' deliverables and services.* *Note 3: The risk sources may vary across the entire product life cycle.*
MAN.7.BP2: Identify cybersecurity events. Identify and regularly evaluate cybersecurity information and derive potential cybersecurity events. Update the relevant assets, damage and threat scenarios with affected parties.
MAN.7.BP3: Analyze risks. Analyze and determine the risk of the potential cybersecurity events based on the impact they may have and based on the feasibility of an attack path to be exploited in order to support prioritization for the treatment of risks. *Note 4: Different methods may be used to analyze technical risks of a system, for example, TARA including attack path analysis, simulation, ETA, ATA, FTA etc.*
MAN.7.BP4: Define risk treatment options. For each risk select a treatment option to retain, reduce, avoid, or transfer (share) the risk.
MAN.7.BP5: Define and perform risk treatment activities. Define and perform risk activities for risk treatment options.

MAN.7.BP6: Monitor risks. Regularly re-evaluate the risks related to the identified potential cybersecurity events to determine changes in the status of the cybersecurity risks, re-evaluate the risk treatment options and review the progress of the risk treatment activities.

Note 5: Risks of high priority may need to be communicated to and monitored by higher levels of management.

MAN.7.BP7: Take corrective action. When risk treatment activities are not effective, take appropriate corrective action.

Note 6: Corrective actions may involve re-evaluation of risks, developing and implementing new mitigation concepts or adjusting the existing concepts.

MAN.7 Cybersecurity Risk Management	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5
Output Information Items					
08-55 Risk treatment			X	X	X
14-02 Corrective action				X	X
15-09 Risk status				X	X
15-51 Analysis results	X	X	X		
17-53 Cybersecurity threat scenario		X			
Base Practices					
BP1: Identify cybersecurity risk management scope	X	X			
BP2: Identify potential cybersecurity events		X			
BP3: Analyze risks			X		
BP4: Define risk treatment options				X	X
BP5: Define and perform risk treatment activities.				X	X
BP6: Monitor risks				X	
BP7: Take corrective action					X

4.3. Cybersecurity Engineering Process Group (SEC)

4.3.1. SEC.1 Cybersecurity Requirements Elicitation

Process ID
SEC.1
Process name
Cybersecurity Requirements Elicitation
Process purpose
The purpose is to specify cybersecurity goals and requirements from the outcomes of cybersecurity risk management covering the threat scenarios.

Process outcomes

1) Cybersecurity goals are specified.
2) Cybersecurity requirements are derived from cybersecurity goals.
3) Consistency and bidirectional traceability are maintained between cybersecurity requirements and goals and between the cybersecurity goals and the threat scenarios.
4) The cybersecurity requirements are agreed and communicated to all affected parties.

Base practices

SEC.1.BP1: Specify cybersecurity goals and cybersecurity requirements. Specify cybersecurity goals for the threat scenarios according to the decisions regarding risk treatment to achieve risk reduction.

Specify functional and non-functional cybersecurity requirements for the cybersecurity goals.

Specify these according to defined characteristics for requirements.

Note 1: This includes the refinement of requirements during iterations of this process.

Note 2: This includes requirements for post-development phases which may include production, operation, maintenance and decommissioning.

Note 3: Characteristics of requirements are defined in standards such as ISO IEEE 29148, ISO 26262-8:2018, or the INCOSE Guide To Writing Requirements.

Note 4: Examples for defined characteristics of requirements shared by technical standards are verifiability (i.e., verification criteria being inherent in the requirements text), unambiguity/comprehensibility, freedom from design and implementation, and not contradicting any other requirements.

SEC.1.BP2: Ensure consistency and establish bidirectional traceability. Ensure consistency and establish bidirectional traceability between the cybersecurity requirements and the cybersecurity goals. Ensure consistency and establish bidirectional traceability between the cybersecurity goals and the threat scenarios.

SEC.1.BP3: Communicate agreed cybersecurity requirements. Communicate agreed cybersecurity requirements to all affected parties.

Note 5: Cybersecurity goals might be communicated as well to provide additional context information for the derived cybersecurity requirements.

SEC.1 Cybersecurity Requirements Elicitation	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Output Information Items				
17-00 Requirement	X	X		
17-54 Requirement Attribute	X	X		
15-51 Analysis Results	X	X		
13-51 Consistency Evidence			X	
13-52 Communication Evidence				X
17-51 Cybersecurity goals	X			

Base Practices				
BP1: Specify cybersecurity goals and cybersecurity requirements.	X	X		
BP2: Ensure consistency and establish bidirectional traceability			X	
BP3: Communicate agreed cybersecurity requirements				X

4.3.2. SEC.2 Cybersecurity Implementation

Process ID
SEC.2
Process name
Cybersecurity Implementation
Process purpose
The purpose is to refine the design of the system, software and hardware, consistent with the cybersecurity requirements and to ensure they are implemented.
Process outcomes
1) The architecture of the system, software, and hardware is refined. 2) Consistency and bidirectional traceability are established between cybersecurity requirements and system architecture, software architecture and components of hardware architecture; consistency and bidirectional traceability are established between cybersecurity requirements and software detailed design and hardware detailed design. 3) Appropriate cybersecurity controls are selected. 4) Weaknesses are analyzed. 5) Detailed design of software and hardware is refined. 6) Consistency and bidirectional traceability are established between the software architecture and software detailed design; and consistency and bidirectional traceability are established between the components of hardware architecture and hardware detailed design. 7) The agreed cybersecurity implementation is communicated to all affected parties.

Base practices
SEC.2.BP1: Refine the details of the architecture. The architecture of the system, software, and hardware is refined based on cybersecurity requirements. *Note 1: Refinement here means to add, adapt, or rework elements of the architectures.*
SEC.2.BP2 Ensure consistency and establish bidirectional traceability for cybersecurity requirements. Ensure consistency and establish bidirectional traceability between cybersecurity requirements and system architecture, software architecture and components of hardware architecture. Ensure consistency and establish bidirectional traceability between cybersecurity requirements and software detailed design and hardware detailed design.
SEC.2.BP3: Select cybersecurity controls. Select appropriate cybersecurity controls to achieve or support the cybersecurity requirements including an explanation of how the related risk is mitigated. *Note 2: Typically, cybersecurity controls are technical measures or other solutions to detect, counteract or mitigate cybersecurity risks.*
SEC.2.BP4: Analyze architecture for weaknesses. Analyze the architecture of the system, software, and hardware, incl. interfaces and detailed design regarding weaknesses to identify

vulnerabilities. Document the design decisions.

SEC.2.BP5: Refine the detailed design. The detailed design is refined based on the architecture of the software and hardware.

Note 3: Refinement here means to add, adapt or rework elements of the detailed design.

SEC.2.BP6: Ensure consistency and establish bidirectional traceability for architecture and detailed design.
Ensure consistency and establish bidirectional traceability between the software architecture and software detailed design. Ensure consistency and establish bidirectional traceability between the components of hardware architecture and hardware detailed design.

SEC.2.BP7: Communicate agreed results of cybersecurity implementation. Communicate the agreed results of the cybersecurity implementation to all affected parties.

Note 4: The communicated contents may include both results of the cybersecurity implementation and vulnerabilities identified within the architecture.

SEC.2 Cybersecurity Implementation	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5	Outcome 6	Outcome 7
Output Information Items							
04-04 Software Architecture	X	X					
04-05 Software Detailed Design		X			X		
04-06 System Architecture	X	X					
04-52 Hardware Architecture	X	X					
04-53 Hardware Detailed Design		X			X		
13-51 Consistency Evidence		X				X	
13-52 Communication Evidence							X
15-50 Vulnerability analysis Evidence				X			
17-52 Cybersecurity controls			X				
Base Practices							
BP1: Refine the details of the architecture	X						
BP2: Ensure consistency and establish bidirectional traceability for cybersecurity requirements		X					
BP3: Select cybersecurity controls			X				
BP4: Analyze architecture for weaknesses				X			
BP5: Refine the detailed design					X		
BP6: Ensure consistency and establish bidirectional traceability for architecture and detailed design						X	
BP7: Communicate agreed results of cybersecurity implementation							X

4.3.3. SEC.3 Risk Treatment Verification

Process ID
SEC.3
Process name
Risk Treatment Verification
Process purpose
The purpose is to confirm that the implementation of the design and integration of the components comply with the cybersecurity requirements, the refined architectural design and detailed design.
Process outcomes
1) Risk treatment verification measures are developed. 2) Verification measures are selected according to the release scope. 3) The implementation of the design and the integration of the components is verified. Verification results are recorded. 4) Consistency and bidirectional traceability are established between the risk treatment verification measures and the cybersecurity requirements, as well as between the risk treatment verification measures and the refined architectural design, detailed design and software units. Bidirectional traceability is established between the verification results and the risk treatment verification measures. 5) The results of the risk treatment verification are summarized and communicated to all affected parties.

Base practices
SEC.3.BP1: Specify risk treatment verification measures. Specify risk treatment verification measures suitable to provide evidence of compliance of the implementation with the cybersecurity requirements and the refined architectural design and detailed design. *Note 1: The risk treatment verification may provide objective evidence that the outputs of a particular phase of the system, software and hardware development life cycle (e.g., requirements, design, implementation, testing) meet the specified requirements for that phase.* *Note 2: The risk treatment verification measures may further include a check for any unspecified functionality, dynamic verification of control flow and data flow, and static analysis focusing on security coding standards.* *Note 3: The risk treatment verification methods and techniques may include network tests simulating attacks (non-authorized commands, signals with wrong hash key, flooding the connection with messages, etc.), and simulating brute force attacks.* *Note 4: The risk treatment verification methods and techniques may also include audits, review, and other techniques.* *Note 5: Methods of deriving test cases for verification measures may include generation and analysis of equivalence classes, boundary values analysis, and/or error guessing based on knowledge or experience.*
SEC.3.BP2: Select verification measures. Document the selection of verification measures considering selection criteria including criteria for regression verification. The documented selection of verification measures shall have sufficient coverage according to the release scope.

Note 6: Examples for selection criteria can be prioritization of requirements, continuous development, the need for regression verification (due to e.g., changes to the software requirements), or the intended use of the delivered product release (test bench, test track, public road etc.)

SEC.3.BP3: Perform risk treatment verification activities. Verify the implementation of the design and component integration using the selected risk treatment verification measures. Record the risk treatment verification results including pass/fail status and corresponding verification measure data.

Note 7: See SUP.9 for handling verification results that deviate from expected results.

SEC.3.BP4: Ensure consistency and establish bidirectional traceability. Ensure consistency and establish bidirectional traceability between the risk treatment verification measures and the cybersecurity requirements. Ensure consistency and establish bidirectional traceability between the risk treatment verification measures and the refined architectural design, detailed design and software units. Establish bidirectional traceability between the verification results and risk treatment verification measures.

Note 8: Bidirectional traceability supports consistency, facilitates impact analysis, and supports demonstration of verification coverage. Traceability alone, e.g., the existence of links, does not necessarily mean that the information is consistent.

SEC.3.BP5: Summarize and communicate results. Summarize the risk treatment verification results and communicate them to all affected parties.

Note 9: Providing all necessary information from the risk treatment verification execution in a summary enables other parties to judge the consequences.

SEC.3 Risk Treatment Verification	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5
Output Information Items					
08-60 Verification Measure	X				
03-50 Verification Measure Data			X		
08-58 Verification Measure Selection Set		X			
15-52 Verification Results			X		
13-51 Consistency Evidence				X	
13-52 Communication Evidence					X
Base Practices					
BP1: Specify risk treatment verification measures	X				
BP2: Select verification measures		X			
BP3: Perform risk treatment verification activities			X		
BP4: Ensure consistency and establish bidirectional traceability				X	
BP5: Summarize and communicate results					X

4.3.4. SEC.4 Risk Treatment Validation

Process ID
SEC.4
Process name
Risk Treatment Validation
Process purpose
The purpose is to confirm that the integrated system achieves the associated cybersecurity goals.
Process outcomes
1) Risk treatment validation measures are specified based on the cybersecurity goals. 2) Validation measures are selected according to defined criteria, including criteria for regression validation. 3) The integrated system is validated using the specified validation measures, and the results of the validation are recorded. 4) Consistency and bidirectional traceability are established between the validation measures and the cybersecurity goals; and bidirectional traceability is established between validation results and validation measures. 5) The results of the risk treatment validation are summarized and communicated to all affected parties.

Base practices
SEC.4.BP1: Specify risk treatment validation measures. Specify the risk treatment validation measures to provide evidence for achievement of the associated cybersecurity goals. *Note 1: Risk treatment validation measures typically use cybersecurity-relevant methods to detect unidentified vulnerabilities (e.g., penetration testing).* *Note 2: Methods of deriving test cases may include generation and analysis of equivalence classes, boundary values analysis, negative tests and/or error guessing based on knowledge or experience.*
SEC.4.BP2: Select validation measures. Document the selection of validation measures according to defined criteria including criteria for regression validation. The documented selection of validation measures shall have sufficient coverage of the cybersecurity goals.
SEC.4.BP3: Perform risk treatment validation activities. Validate the integrated system using the selected risk treatment validation measures. Record the validation results and corresponding validation measure data. *Note 3: See SUP.9 for handling validation results that deviate from expected results.*
SEC.4.BP4: Ensure consistency and establish bidirectional traceability. Ensure consistency and establish bidirectional traceability between risk treatment validation measures and cybersecurity goals. Establish bidirectional traceability between validation results and validation measures. *Note 4: Bidirectional traceability supports consistency, facilitates impact analysis, and supports demonstration of validation coverage. Traceability alone, e.g., the existence of links, does not necessarily mean that the information is consistent.*
SEC.4.BP5 Summarize and communicate results. Summarize the risk treatment validation results and communicate them to all affected parties.

Note 5: This may include information from the risk treatment validation activities and important findings concerning additional vulnerabilities to enable other parties to judge the consequences.

SEC.4 Risk Treatment Validation	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5
Output Information Items					
08-59 Validation Measure	X				
03-55 Validation Measure Data			X		
08-57 Validation Measure Selection Set		X			
13-24 Validation Results			X		
13-51 Consistency Evidence				X	
13-52 Communication Evidence					X
Base Practices					
BP1: Specify risk treatment validation measures	X				
BP2: Select validation measures		X			
BP3: Perform risk treatment validation activities			X		
BP4: Ensure consistency and establish bidirectional traceability				X	
BP5: Summarize and communicate results					X

Annex A – Process Assessment and Reference Model Conformity

The given process assessment and reference model is in line with the declarations and definitions in the Automotive SPICE® 4.0 core model. Therefore, the conformity statement given in annex A of the Automotive SPICE®.

Process Reference and Process Assessment Model (Version 4.0) applies. [Automotive Spice® 4.0]

Annex B – Information Item Characteristics

Characteristics of information items are defined using the schema in Table B.1. See Section 3.3.2 of Automotive SPICE® 4.0 on the definition and explanation on how to interpret information items and their characteristics.

Table B.1 — Structure of Information Item Characteristics (IIC)

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 use these in evaluating the samples provided by the organizational unit. It is not intended to use the listed characteristics as a checklist. Some characteristics may be contained in other work products, if found to be appropriate for the assessed organization.

Table B.2 — Information Item Characteristics

This table contains only the relevant information item characteristics for the Automotive SPICE® for Cybersecurity.

ID	Name	Characteristics
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 stakeholders and contacts - tailoring agreements - customer/supplier responsibilities (e.g., roles, RASIC chart) for distributed 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

ID	Name	Characteristics
		duration of supplier's support and maintenance
03-50	Verification measure data	• Verification measure data are data recorded during the execution of a verification measure, e.g.: - for test cases: raw data, logs, traces, tool generated outputs - measurements: values - calculations: values - simulations: protocol - reviews such as optical inspections and findings record - analyses: values
03-55	Validation measure data	• Validation measure data are data recorded during the execution of a validation measure, e.g.: Logs, traces, raw data, crash dumps, review protocols.
04-04	Software architecture	• A justifying rationale for the chosen architecture. • Individual functional and non-functional behavior of the software components • 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.
04-52	Hardware architecture	• Describes the initial floor plan and the overall hardware structure • Identifies the required hardware components • Includes the rationale for chosen options of hardware architecture

ID	Name	Characteristics
		• Identifies own developed and supplied hardware components • Identifies the required internal and external hardware component interfaces • Specifies the interfaces of the hardware components • Specifies dynamic behavior • Identifies the relationship and dependency between hardware components • Describes all hardware variants to be developed • Describes power supply, thermal and grounding concepts
04-53	Hardware detailed design	• Describes the interconnections between the hardware parts • Specifies the interfaces of the hardware parts • Specifies the dynamic behavior (examples are: transitions between electrical states of hardware parts, power-up and power-down sequences, frequencies, modulations, signal delays, debounce times, filters, short circuit behavior, self-protection) • Describes the conclusions and decisions based on e.g., analysis reports, datasheets, application notes • Describes the constraints for layout
08-55	Risk treatment	• Identifies - the risk to be mitigated, avoided, retained or transferred (shared) - the activities to mitigate, avoid, retain or transfer (share) 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/retain/ transfer (share) - alternative descriptions - recommended alternative(s) • justifications
08-57	Validation measure selection set	• Include criteria for re-validation in the case of changes (regression). • Identification of validation measures, also for regression
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

ID	Name	Characteristics
		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
12-01	Request for quotation	• Reference to the requirements specifications • Cybersecurity responsibilities of the supplier • The scope of work regarding cybersecurity, including the cybersecurity goals or the set of relevant cybersecurity requirements and their attributes • Action plan for identified deviations and risks • Identifies desired characteristics, such as: - system architecture, configuration requirements or the requirements for service (consultants, maintenance, etc.) - quality criteria or requirements - project schedule requirements - expected delivery/service dates - cost/price expectations - regulatory standards/requirements • Identifies submission constraints: - date for resubmission of the response • requirements with regard to the format of response
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
13-51	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 - reviewing by peers, e.g., spot checks - maintaining revision history 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.*
13-52	Communication evidence	• All forms of interpersonal communication such as - e-mails, also automatically generated ones - tool-supported workflows - meeting, verbally or via meeting minutes (e.g., daily standups) - podcast - blog - videos - forum - live chat - wikis - photo protocol

ID	Name	Characteristics
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
15-09	Risk status	• Identifies the status, or the change, of an identified risk: - risk statement - risk source - risk impact and risk likelihood - categories and risk thresholds, e.g., for prioritization or setting a status - risk treatment activities in progress
15-21	Supplier evaluation	• States the purpose of evaluation • Identifies supplier selection criteria • 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
15-50	Vulnerability analysis evidence	• Identifies - ID - description - attack path concerned • attack feasibility (e.g., CVSS (Common Vulnerability Scoring System) rating)
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 - 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
17-00	Requirement	• An expectation of functions and capabilities (e.g., non-functional requirements), or one of its interfaces - from a black-box perspective

ID	Name	Characteristics
		- 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 of 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 of 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 - 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 it is necessary to protect by means of cybersecurity • This may include - Confidentiality needs - Authorization needs - Integrity needs - Availability needs - etc. • Information that can be included in the goals: - Goal Title - Objective - Scope - Key Metrics and success criteria - Milestones (if Applicable) - Action plan (if applicable) - stakeholders involved - link to potential risks - budget and resources - Timeline - Compliance and standards - Sign-off and approval

ID	Name	Characteristics
17-52	Cybersecurity controls	• Technical solutions to prevent, detect, or mitigate cybersecurity risks • Associated to one or more cybersecurity requirements
17-53	Cybersecurity threat scenario	• Description of how threats exploit a weakness/vulnerability or multiple weaknesses/vulnerabilities exposing assets to harm, to enable the corresponding risk analysis • Detailed chronological and functional description of an actual or hypothetical threat or group of threats • Sequence of actions that involve interaction with system resulting in a threat scenario • A threat scenario shall include, e.g. - asset targeted by the threat - cybersecurity property which is compromised - compromise cause of the cybersecurity property • Threat scenarios give a detailed and concrete description of applicable threats, like: - ransomware - phishing - spoofing - denial of service
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.* •
18-50	Supplier evaluation criteria	• Expectations for conformity, to be fulfilled by suppliers • Links from the expectations to national/international/domain-specific standards/laws/regulations • Requirements' conformity evidence to be provided by the potential suppliers or assessed by the acquiring organization • agreed exceptions to the requirements

Annex C – Terminology

Automotive SPICE® follows the following precedence for use of terminology:

a) ISO/IEC 33001 for assessment-related terminology
b) ISO/IEC/IEEE 24765 and ISO/IEC/IEEE 29119 terminology (as contained in Annex C)
c) Terms introduced by Automotive SPICE® (as contained in Annex C)
d) ISO/SAE 21434 for cybersecurity-related terminology

Annex C lists the applicable terminology references from ISO/IEC/IEEE 24765 and ISO/IEC/IEEE 29119. It also provides terms which are specifically defined within Automotive SPICE®. Some of these definitions are based on ISO/IEC/IEEE 24765.

Table C.1 — Terminology

Term	Origin	Description
Acceptance testing	ISO/IEC/IEEE 24765	Formal testing conducted to enable a user, customer, or authorized entity to determine whether to accept a system or component.
Application parameter	Automotive SPICE® 4.0	An application parameter is a software variable containing data that can be changed at the system or software levels; they influence the system or software behavior and properties. The notion of application parameter is expressed in two ways: • The specification (including variable names, the domain value range, technical data types, default values, physical unit (if applicable), the corresponding memory maps, respectively). • The actual quantitative data value it receives by means of data application. Application parameters are not requirements. They are a technical implementation solution for configurability-oriented requirements.
Architecture element	Automotive SPICE® 4.0	Result of the decomposition of the architecture on system and software level: • The system is decomposed into elements of the system architecture across appropriate hierarchical levels. • The software is decomposed into elements of the software architecture across appropriate hierarchical levels down to the software components (the lowest level elements of the software architecture).
Asset	ISO/SAE 21434	Object that has value or contributes to value.
Attack path	ISO/SAE 21434	Set of deliberate actions to realize a threat scenario.
Attack feasibility	ISO/SAE 21434	Attribute of an attack path describing the ease of successfully carrying out the corresponding set of actions.
Black-box testing	Automotive SPICE® 4.0	Method of requirement testing where tests are developed without knowledge of the internal structure and mechanisms of the tested item.
Code review	Automotive SPICE® 4.0	A check of the code by one or more qualified persons to determine its suitability for its intended use and identify discrepancies from specifications and standards.
Coding	ISO/IEC/IEEE 24765	The transforming of logic and data from design specifications (design descriptions) into programming language.

Consistency	Automotive SPICE® 4.0	Consistency addresses content and semantics and ensures that work products are not in contradiction to each other. Consistency is supported by bidirectional traceability.
Cybersecurity event	ISO/SAE 21434	cybersecurity information that is relevant for an item or component
Cybersecurity goal	ISO/SAE 21434	Concept-level cybersecurity requirement associated with one or more threat scenarios.
Cybersecurity information	ISO/SAE 21434	information with regard to cybersecurity for which relevance is not yet determined
Cybersecurity property	ISO/SAE 21434	Attribute that can be worth protecting.
Damage scenario	Automotive SPICE® 4.0	Adverse consequence involving a vehicle or vehicle function and affecting a stakeholder.
Element	Automotive SPICE® 4.0	Elements are all structural objects on architectural and design level on the left side of the "V". Such elements can be further decomposed into more fine-grained sub-elements of the architecture or design across appropriate hierarchical levels.
Error	ISO/IEC/IEEE 24765	The difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.
Fault	ISO/IEC/IEEE 24765	A manifestation of an error in software.
Functional requirement	ISO/IEC/IEEE 24765	A statement that identifies what a product or process must accomplish to produce required behavior and/or results.
Hardware	ISO/IEC/IEEE 24765	Physical equipment used to process, store, or transmit computer programs or data.
Integration	Automotive SPICE® 4.0	A process of combining items to larger items up to an overall system.
Item	ISO 21434	component or set of components that implements a function at the vehicle level
Quality assurance	ISO/IEC/IEEE 24765	A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements.
Regression testing	Automotive SPICE® 4.0	Selective retesting of a system or item to verify that modifications have not caused unintended effects and that the system or item still complies with its specified requirements.
Requirement	Automotive SPICE® 4.0	A property or capability that must be achieved or possessed by a system, system item, product or service to satisfy a contract, standard, specification or other formally imposed documents.
Requirements specification	Automotive SPICE® 4.0	A document that specifies the requirements for a system or item. Typically included are functional requirements, performance requirements, interface requirements, design requirements, and development standards.
Software	ISO/IEC/IEEE 24765	Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system.
Software component	Automotive SPICE® 4.0	Software component in design and implementation-oriented processes:

		The software architecture decomposes the software into software components across appropriate hierarchical levels down to the lowest-level software components in a conceptual model. Software component in verification-oriented processes: The implementation of a SW component under verification is represented e.g., as source code, object files, library file, executable, or executable model.
Software element	Automotive SPICE® 4.0	Refers to software component or software unit
Software unit	Automotive SPICE® 4.0	Software unit in design and implementation-oriented processes: As a result of the decomposition of a software component, the software is decomposed into software units which are a representation of a software element, which is decided not to be further subdivided and that is a part of a software component at the lowest level, in a conceptual model. Software unit in verification-oriented processes: An implemented SW unit under verification is represented e.g., as source code files, or an object file.
Static analysis	Automotive SPICE® 4.0	A process of evaluating an item based on its form, structure, content or documentation.
System	Automotive SPICE® 4.0	A collection of interacting items organized to accomplish a specific function or set of functions within a specific environment.
Testing	Automotive SPICE® 4.0	Activity in which an item (system, hardware, or software) is executed under specific conditions; and the results are recorded, summarized and communicated.
Threat scenario	ISO/SAE 21434	Potential cause of compromise in cybersecurity properties of one or more assets in order to realize a damage scenario.
Traceability	ISO/IEC/IEEE 24765	The degree to which a relationship can be established between two or more products of the development process, especially products having a predecessor-successor or master-subordinate relationship to one another.
Unit	Automotive SPICE® 4.0	Part of a software component which is not further subdivided. → [SOFTWARE COMPONENT]
Unit test	Automotive SPICE® 4.0	The testing of individual software units or a set of combined software units.
Validation	ISO/IEC/IEEE 29119	Validation demonstrates that the work item can be used by the users for their specific tasks.
Verification	ISO/IEC/IEEE 29119	Verification is confirmation, through the provision of objective evidence, that specified requirements have been fulfilled in a given work item.
Vulnerability	ISO/SAE 21434	Weakness that can be exploited as part of an attack path.
Weakness	ISO/SAE 21434	Defect or characteristic that can lead to undesirable behavior.
White-box testing	Automotive SPICE® 4.0	Method of testing where tests are developed based on the knowledge of the internal structure and mechanisms of the tested item.

Table C.2 — Abbreviations

AS	**A**utomotive **SPICE**
ACSMS	**A**utomotive **C**ybersecurity **M**anagement **S**ystem

ATA	**A**ttack **T**ree **A**nalysis
BP	**B**ase **P**ractice
CAN	**C**ontroller **A**rea **N**etwork
CASE	**C**omputer-**A**ided **S**oftware **E**ngineering
CCB	**C**hange **C**ontrol **B**oard
CFP	**C**all **F**or **P**roposals
CPU	**C**entral **P**rocessing **U**nit
ECU	**E**lectronic **C**ontrol **U**nit
EEPROM	**E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory
FMEA	**F**ailure **M**ode and **E**ffects **A**nalysis
FTA	**F**ault **T**ree **A**nalysis
GP	**G**eneric **P**ractice
GR	**G**eneric **R**esource
HARA	**H**azard **A**nalysis and **R**isk **A**ssessment
IEC	**I**nternational **E**lectrotechnical **C**ommission
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
I/O	**I**nput/**O**utput
ISO	**I**nternational **O**rganization for **S**tandardization
MISRA	**M**otor **I**ndustry **S**oftware **R**eliability **A**ssociation
OII	**O**utput **I**nformation **I**tem
PA	**P**rocess **A**ttribute
PAM	**P**rocess **A**ssessment **M**odel
PRM	**P**rocess **R**eference **M**odel
RAM	**R**andom **A**ccess **M**emory
RC	**Rec**ommendation
RL	**Ru**le
ROM	**R**ead **O**nly **M**emory
SPICE	**S**oftware-based systems **P**rocess **I**mprovement and **C**apability d**E**termination
TARA	**T**hreat **A**nalysis and **R**isk **A**ssessment
UNECE	**U**nited **N**ations **E**conomic **C**ommission for **E**urope
VDA	**V**erband **D**er **A**utomobilindustrie (German Association of the Automotive Industry)

Annex D – Traceability and Consistency

Traceability and consistency are addressed by a single base practice in the Automotive SPICE® for Cybersecurity as well as in the Automotive SPICE® 4.0.

Traceability refers to the existence of references or links between work products, thereby further supporting coverage, impact analysis, requirements implementation status tracking, etc. In contrast, consistency addresses content and semantics.

Furthermore, bidirectional traceability has been explicitly defined between

- threat scenarios and cybersecurity goals,
- cybersecurity goals and validation specification,
- cybersecurity requirements/architecture/software detailed design/hardware detailed design and risk treatment verification specification,
- validation specifications and validation results, and
- verification measures and verification results.

An overview of bidirectional traceability and consistency is depicted in the following figure.

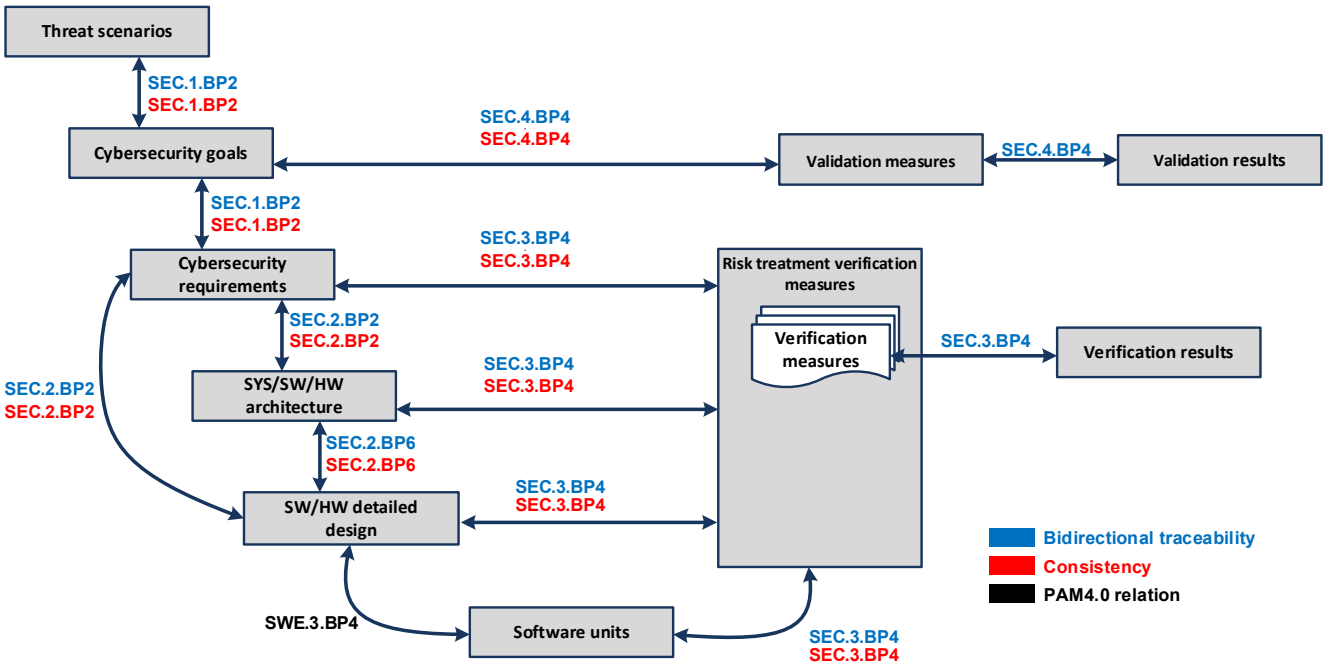

Figure 5 — Bidirectional Traceability and Consistency

Annex E– General Concept of Automotive SPICE® for Cybersecurity

In this Annex the relationship between Automotive SPICE® for Cybersecurity and ISO/SAE 21434 is described. Figure 7 shows the base practices of Automotive SPICE® for Cybersecurity with the respective IIC or work products and the respective requirement [RQ] in the ISO/SAE 21434.

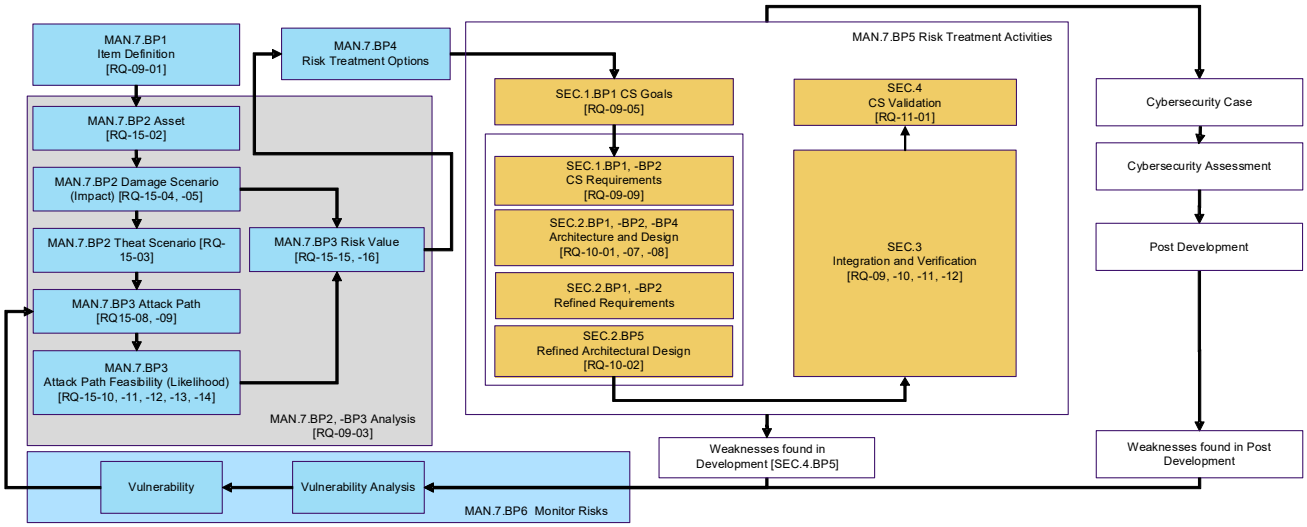

Figure 6 — Automotive SPICE® for Cybersecurity general concept