VDA QMC

Verband der Automobilindustrie
Qualitäts-Management-Center

Joint Quality Management in the Supply Chain

Automotive SPICE® for Cybersecurity

Part I: Process Reference and Assessment Model for Cybersecurity Engineering

Part II: Rating Guidelines on Process Performance (Level 1) for Cybersecurity Engineering

2nd edition, December 2024

Joint Quality Management in the Supply Chain

Automotive SPICE® for Cybersecurity

Part I: Process Reference and Assessment Model for Cybersecurity Engineering

Part II: Rating Guidelines on Process Performance (Level 1) for Cybersecurity Engineering

2nd edition, December 2024
Verband der Automobilindustrie e. V. (VDA)

Non-Binding VDA Standard Recommendation

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

Exclusion of Liability

VDA volumes are recommendations available for general use. Anyone applying them is responsible for ensuring they are used correctly in each case.

This VDA volume takes into account the state of knowledge and technology prevailing at the time of publication. Implementation of VDA recommendations does not absolve anyone of responsibility for their own actions. Every user is accountable for their own behavior. Liability on the part of the VDA and those involved in preparing VDA recommendations is excluded.

If during the use of VDA recommendations errors or the possibility of misinterpretation are found, it is requested that these be reported to the VDA immediately for correction (if required).

Copyright

Translations

This publication will also be issued in other languages. The available versions can be downloaded from the Automotive SPICE® – VDA QMC (vda-qmc.de) website.

Copyright Notice

Trademark

Table of Contents

List of Figures

List of Tables

Introduction

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, when used with an appropriate assessment method, which helps to identify process-related product risks. 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).

Part I of 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 including at least system and software process group. Otherwise, an assessment using both the Automotive SPICE for Cybersecurity PAM and Automotive SPICE PAM for the VDA scope processes has to be performed.

Part II of this document complements the existing Automotive SPICE Guideline (2nd edition). It contains interpretation and rating guidelines for the processes defined in Part I. Chapters 1 "Application and interpretation of rating guidelines" and 2 "Key concepts and overall guidelines" of the Automotive SPICE Guideline (2nd edition) also apply to Part II and therefore are not repeated here.

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.

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® 4.0is 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.

Relation to ISO/SAE 21434

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

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

Certain aspects of the 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 the 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 is 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 including Guideline 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

Requirements on Assessment Scope

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

When assessing the entire process profile using an existing assessment, the processes from SUP process group need not to be re-evaluated. In cases when 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. So, the cybersecurity goals are also covering unintended use. This is either done in the actual environment or a simulated environment.

Cybersecurity validation on the other hand is the proof that the unintended use of the product is prevented. The validation ensures that the expectation of the receiving party of the delivered product is fulfilled.

ACQ.2 is described as process once performed in 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 scope.

Part I Process Reference and Assessment Model for Cybersecurity Engineering

1 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 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:

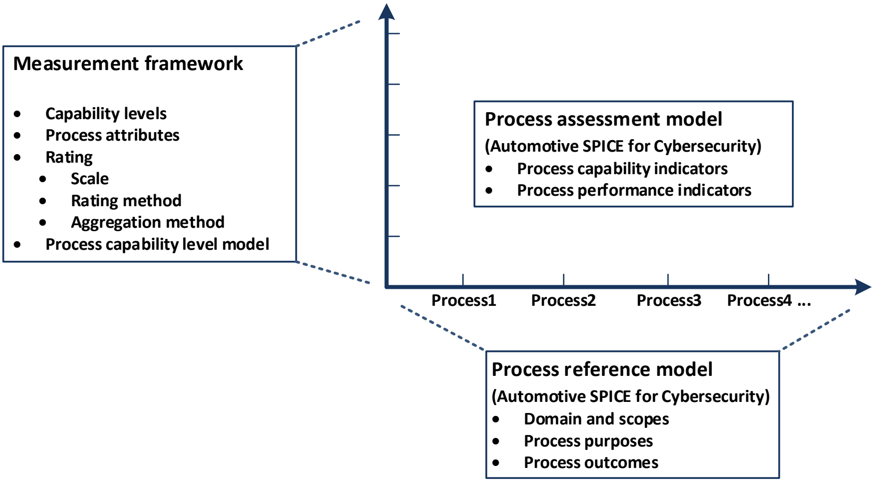


Figure 1 — Process Assessment Model Relationship

1.1 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 life cycle processes, Organizational life cycle processes and Supporting life cycle 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.

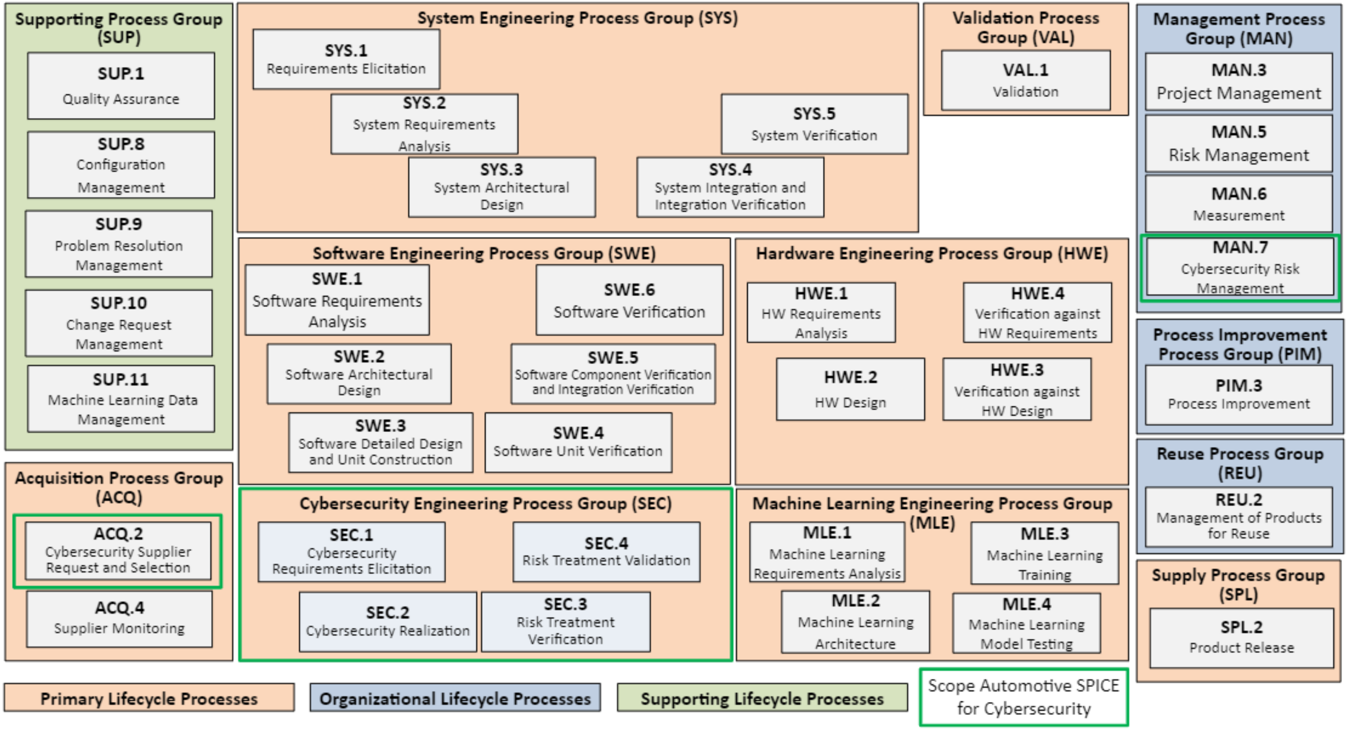

Supporting Process Group (SUP)
SUP.1 Quality Assurance
SUP.8 Configuration Management
SUP.9 Problem Resolution Management
SUP.10 Change Request Management
SUP.11 Machine Learning Data Management
System Engineering Process Group (SYS)
SYS.1 Requirements Elicitation
SYS.2 System Requirements Analysis
SYS.3 System Architectural Design
SYS.4 System Integration and Integration Verification
SYS.5 System Verification
Validation Process Group (VAL)
VAL.1 Validation
Management Process Group (MAN)
MAN.3 Project Management
MAN.5 Risk Management
MAN.6 Measurement
MAN.7 Cybersecurity Risk Management
Software Engineering Process Group (SWE)
SWE.1 Software Requirements Analysis
SWE.2 Software Architectural Design
SWE.3 Software Detailed Design and Unit Construction
SWE.4 Software Unit Verification
SWE.5 Software Component Verification and Integration Verification
SWE.6 Software Verification
Hardware Engineering Process Group (HWE)
HWE.1 HW Requirements Analysis
HWE.2 HW Design
HWE.3 Verification against HW Design
HWE.4 Verification against HW Requirements
Process Improvement Process Group (PIM)
PIM.3 Process Improvement
Acquisition Process Group (ACQ)
ACQ.2 Cybersecurity Supplier Request and Selection
ACQ.4 Supplier Monitoring
Cybersecurity Engineering Process Group (SEC)
SEC.1 Cybersecurity Requirements Elicitation
SEC.2 Cybersecurity Realization
SEC.3 Risk Treatment Verification
SEC.4 Risk Treatment Validation
Machine Learning Engineering Process Group (MLE)
MLE.1 Machine Learning Requirements Analysis
MLE.2 Machine Learning Architecture
MLE.3 Machine Learning Training
MLE.4 Machine Learning Model Testing
Reuse Process Group (REU)
REU.2 Management of Products for Reuse
Supply Process Group (SPL)
SPL.2 Product Release
Primary Lifecycle Processes
Organizational Lifecycle Processes
Supporting Lifecycle Processes
Scope Automotive SPICE for Cybersecurity

Figure 2 — Automotive SPICE and Automotive SPICE for Cybersecurity Process Reference Model – Overview

1.1.1 Primary Life Cycle Processes category

The primary life cycle 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 life cycle 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 Life Cycle Processes – SEC

1.1.2 Organizational Life Cycle Processes category

The Organizational Life Cycle 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 Life Cycle Processes category consists of the following groups:

- the Management Process Group
- the Process Improvement Process Group
- the Reuse 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

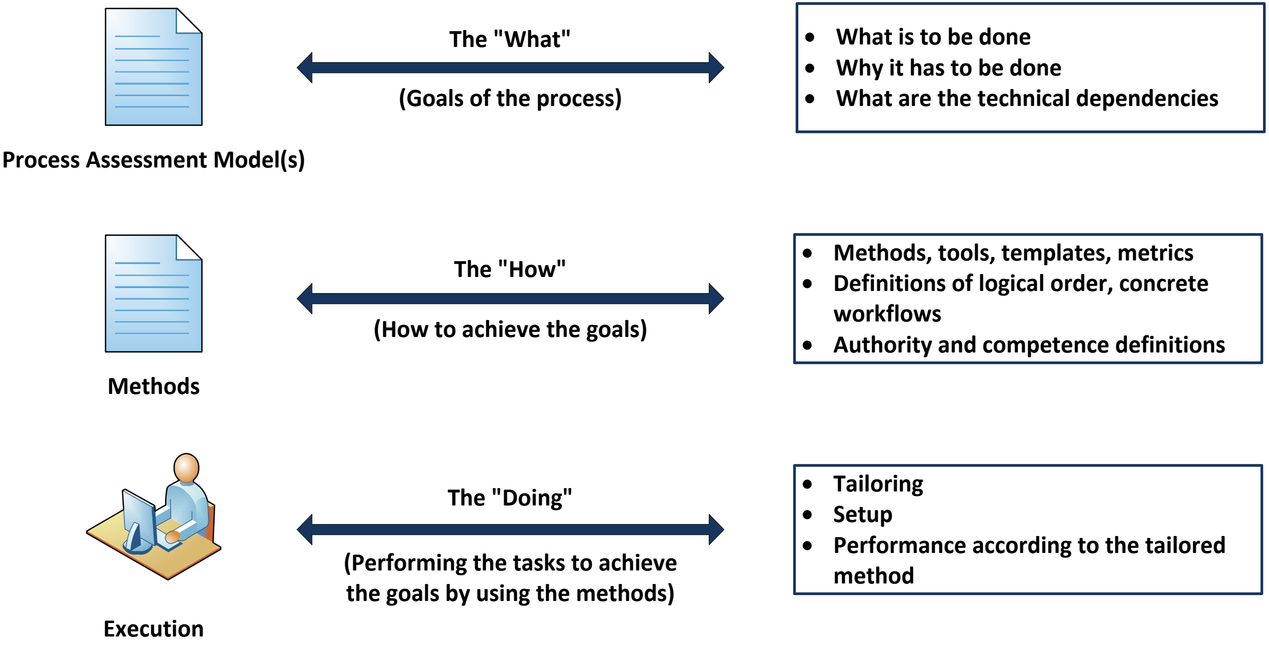
Table 3 — Organizational Life Cycle Processes – MAN

1.2 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.

1.3 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.



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
- Authority and competence definitions

Execution

The "Doing"

(Performing the tasks to achieve the goals by using the methods)

- Tailoring
- Setup
- Performance according to the tailored method

Figure 2 — 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.

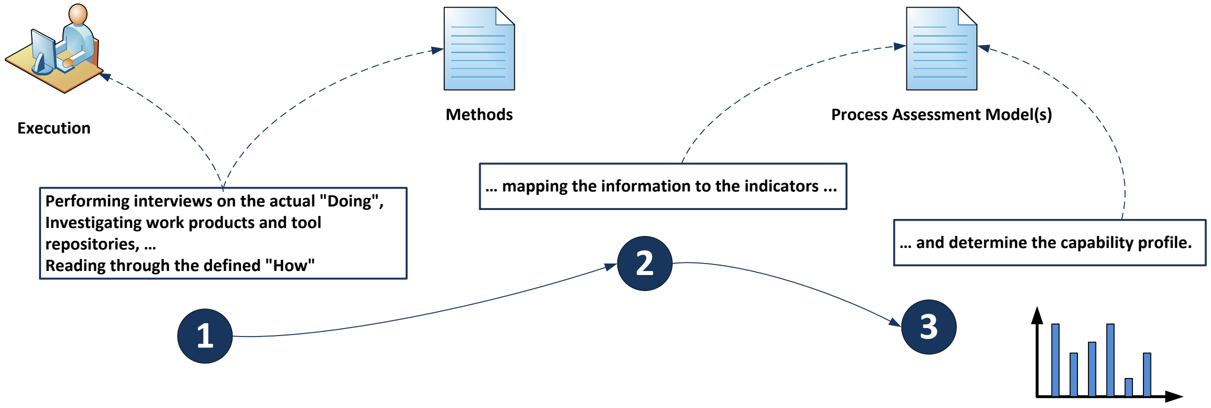

Execution
Methods
Process Assessment Model(s)
Performing interviews on the actual "Doing", Investigating work products and tool repositories, ... Reading through the defined "How"
... mapping the information to the indicators ...
... and determine the capability profile.
1
2
3

Figure 3 — Performing a Process Assessment for Determining Process Capability

2 Process Reference Model and Performance Indicators (Level 1)

2.1 Acquisition Process Group (ACQ)

2.1.1 ACQ.2 Supplier Request and Selection

Process ID

ACQ.2

Process name

Supplier Request and Selection

Process purpose

The purpose is to award 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, action, and risk measures 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 organization's capability of the supplier 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 any previous projects ad*

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*
- *Experiences 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 share, 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 measure				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

2.2 Management Process Group (MAN)

2.2.1 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, attack feasibility rating in order to support prioritization for the treatment of risks. 4) Cybersecurity risk measures are defined, applied, and assessed to determine changes in the status of risk and the progress of the risk treatment activities. 5) Appropriate treatment is taken to mitigate the impact of risk based on its priority, probability, 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 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 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, attack path analysis, simulation, TARA, FTA etc.

MAN.7.BP4: Define risk treatment options. For each risk select a treatment option to retain, reduce, avoid, share or transfer 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 risk related to the identified potential cybersecurity events to determine changes in the status of a cybersecurity risk, 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 measure			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

2.3 Cybersecurity Engineering Process Group (SEC)

2.3.1 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 and ensure consistency between the threat scenarios, cybersecurity goals and cybersecurity requirements.
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 with risk treatment decision avoidance or 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 goals and cybersecurity requirements to all affected parties.

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

2.3.2 SEC.2 Cybersecurity Implementation

Process ID
SEC.2
Process name
Cybersecurity Implementation
Process purpose
The purpose is to refine design of the system, software, and hardware, consistent with the cybersecurity requirements and 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; and consistency and bidirectional traceability are established between cybersecurity requirements and software detailed design and hardware detailed design. 3) Appropriate cybersecurity controls are selected. 4) Vulnerabilities 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 risk treatment 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 goals and 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 on how the related risk is mitigated.

Note 2: Typically, cybersecurity controls are technical or other solutions to avoid, detect, counteract or mitigate cybersecurity risks.

SEC.2.BP4: Analyze architecture for vulnerabilities. Analyze the architecture of the system, software, and hardware, incl. interfaces and detailed design, to identify and analyze 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 components 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 are established 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 vulnerabilities				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

2.3.3 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 check for any unspecified functionalities, control flow and data flow verification, 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 according 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, and 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 with each other.

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			
13-25 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

2.3.4 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 considering 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 follow 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 considering selection 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, and 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 with each other.

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

Part II Rating Guidelines on Process Performance (Level 1) for Cybersecurity Engineering

3 ACQ.2 Supplier Request and Selection

The purpose is to award a supplier with a contract/agreement based on relevant criteria.

The main requirement for distributed cybersecurity activities is to issue request for quotations for cybersecurity-relevant services and products.

The customer in the supplier request and selection process identifies use cases of supplier involvements and the relationships with suppliers. Supplier evaluation and selection criteria are defined and need to be applied at least in the following use cases:

- Supplier develops a component on the base of customer requirements (e.g., engineering service)
- Supplier delivers and maintains a component that is provided off-the-shelf to the customer (e.g., operating system, device drivers, system with hard- and software)
- Supplier delivers a component created based on the customer's requirements and contains off-the-shelf (sub-) components
- Excluded are suppliers that deliver products without any support (e.g., free and open source software)

3.1 General Information

3.1.1 Evaluation criteria for cybersecurity

In cases of cybersecurity-relevant services and products, the evaluation criteria should include cybersecurity-relevant supplier criteria, such as a certified Cybersecurity Management System, capability profile of an Automotive SPICE for Cybersecurity assessment, cybersecurity best practices from previous projects, etc.

[ACQ.2.RL.1] If cybersecurity-relevant services and products are requested and cybersecurity capabilities are not covered in the evaluation criteria, the corresponding indicator BP1 shall be downrated.

3.1.2 Evidence of corrective actions

In cases of cybersecurity relevant services and products where the evaluation criteria are not fulfilled corrective actions shall be defined in the agreed action plan

[ACQ.2.RL.2] If cybersecurity-relevant services and products are requested and evaluation criteria are not met and there are no corrective actions defined the indicators BP3 and BP4 shall be downrated.

3.2 Rating rules within the process

None.

3.3 Rating rules with other processes at level 1

None.

4 MAN.7 Cybersecurity Risk Management

The purpose is to regularly identify, analyze, prioritize, and monitor risks of damage to relevant stakeholders.

The Cybersecurity Risk Management Process includes a systematic identification of potential cybersecurity events in all phases of product life cycle. Potential cybersecurity events are analyzed for their impact and the feasibility of an attack to evaluate the cybersecurity risk assigned to it.

The analysis can either be structural, numerical, or a combination.

Risk management prepares the risk treatment options based on the determination of risk, damage, and threat. Such risk treatment options can be acceptance, avoidance, mitigation, or transfer (share) of risks.

4.1 General information

4.1.1 Identify cybersecurity risk management scope

To identify the cybersecurity risk management scope, it has to be defined:

- The item
- The functions of the item
- The boundaries of the item
- The operational environment of the item (including interfaces)
- Affected parties

The scope definition may include depending on the product:

a) ***Assets:*** Products, their components and system/software elements are related to assets intended for protection from cybersecurity events within the project.
b) ***Damage scenarios*** to be managed and controlled
c) *Cybersecurity* ***properties*** are for example:
    - Confidentiality
    - Integrity
    - Availability
    - further properties defined in ISO 21434
d) ***Relevant stakeholders*** that could be affected by the adverse consequences of cybersecurity events, e.g.:
    - Road user (e.g., vehicle occupants)
    - Customer of the assessed organization
    - Supplier of the assessed organization
e) The ***impact categories*** are related to the adverse consequences they can cause to relevant stakeholders. Impact categories include, but are not limited to:
    - Safety – e.g., for vehicle occupants
    - Privacy – e.g., driver personal information
    - Financial – e.g., customers service network or financial damage the road user might not overcome
    - Operational – e.g., an impairment of an important vehicle function or impact on infrastructure within manufacturing of customer, etc.
f) ***Life cycle phases*** to be evaluated for the asset:
    - Innovation or demonstrator builds
    - Pre-development
    - Development
    - Production
    - Maintenance and service
    - Decommissioning

The scope definition should represent a minimum definition, including initial damage scenarios. Later identified damage scenarios should not be considered as incomplete scope definition.

Integration of off-the-shelf components should be included within the scope definition of the item, its boundaries, and its interfaces (e.g., free and open source software).

Rating Rules:

> **[MAN.7.RL.1]**: If the risk management scope is not revised on a regular basis the indicator BP1 shall not be rated higher than P.
>
> **[MAN.7.RL.2]**: If the risk management scope does not consider relevant assets (aspects a and c) that are significant for a process-related product risk, BP1 shall not be rated higher than P.
>
> **[MAN.7.RL.3]:** If the scope does not consider the road user as stakeholder (aspect d), BP1 shall not be rated higher than P.

4.1.2 Identify cybersecurity events

Identify and evaluate cybersecurity information and derive cybersecurity events by risk management practices.

Risk management practices should include the methods, roles, tools, review, and release criteria of, for example:

a) Potential risks identification: Repositories and practices for identification and documentation of threat scenarios and damage scenarios:

    - Assessment scheme to inspect structured threat modeling practices of spoofing, tempering, repudiation, information disclosure, denial of service, and elevation of privileges (STRIDE)

- Attack path analysis
- Brainstorming

b) Risk analysis: Repositories and practices for attack path analysis and attack feasibility evaluation:
  - Inductive approach – e.g., with reengineering of knowledge
  - Deductive approach – e.g., with an attack tree analysis
  - Numerical analysis methods, like a common vulnerability scoring system

c) Weighting and rating practices:
  - Scaling and rating methods
  - Weighing criteria, such as the selection of heatmap variants
  - Usage of Cybersecurity Assurance Level (CAL).

d) Risk breakdown within process:
  - Expert boards
  - Roles involved, RASIC
  - Unique identification and traceability of related items

e) Related internal and external interfaces:
  - Sources and practices for current and historical data evaluation
  - Criteria for monitoring
  - Verification of accepted risks
  - Sub-supplier and contractor cooperation

f) Corrective action management:
  - Internal dependencies of the project
  - External dependencies of the project

Rating Rules:

None.

4.1.3 Potential risk analysis and risk determination

The analysis of risks is the basis for selecting a suitable treatment option and all subsequent actions. Cybersecurity risks are subject to change. This makes documentation of risk assumptions and constraints necessary. The analysis of a risk shall include the sequence of actions that can lead to the identification and its exploitation, and an evaluation of each action´s individual likelihood. This analysis for sequences of actions is called Attack Path Analysis for Cybersecurity Risk Management.

Attack path analysis can be performed in the form of:

a) Attack potential analysis:
The expertise, item knowledge, window of opportunity, equipment, and elapsed time are evaluated separately with a final feasibility level aggregation, or

b) Attack vector analysis:
Describes four feasibility ratings depending on the logical and physical distance of exploits. Attack vector analysis may also be included for evaluation of a cybersecurity assurance level (CAL), or

c) Numerical analysis:
Considers several aspects of a and b with defined, model-specific numbers and calculation algorithm.

d) A tailored combination of a–c.

The attack path analysis can be supported by research, experience, and historical data to evaluate and verify the ease of exploitation. Such intelligence data can come from:

e) Automotive Cybersecurity Management System (ACSMS) – e.g., the vulnerability data of former projects, disclosure programs, and shared information.

f) External intelligence service providers – e.g., test centers

g) Information Sharing and Analysis Centers (ISAC)

h) Simulation

All attack paths that create a risk are to be considered. Within the risk analysis, further attack paths might be identified that could lead to other – even unidentified – threats and damage scenarios. The analysis shall ensure these risks are similarly considered, including reasonable prioritization, if necessary.

The resulting cybersecurity risk of a threat scenario can be expressed by different levels and shall result from cybersecurity risk determination – the evaluation of the impact and the related attack feasibility within the context of the project.

Rating Rules:

> **[MAN.7.RL.4]** If none of the described approaches (aspects a–d) for attack path analysis is observable in the assessed project, BP3 shall be downrated.
>
> **[MAN.7.RL.5]** If the cybersecurity risk analysis does not evaluate the ease of exploitation, the indicator BP5 shall be downrated.

4.1.4 Define risk treatment options

For each risk or set of risks, a risk treatment option should be selected (risk treatment decision):

a) Avoidance of risk – e.g., the attack path is made impossible.
b) Reduction of risk – e.g., the feasibility of the attack path is decreased.
c) Transfer (share) of risk – e.g., to assign resources with higher knowledge on avoidance or reduction of the risk.
d) Retainment of risk – e.g., if the risk cannot be lowered any more, it is kept unmitigated.

The risk treatment options can be consecutive and overlapping, since a risk can have multiple attack paths in which each is treated individually through different phases of the project. The elements of one attack path can have different owners and interfaces that require individual treatment options.

Limitation to the traceability of risk options shall be included within the risk treatment decision process. Limitations might result, for example, from the use of a platform solution, free and open source software, or supplied software. In addition, those restrictions may result from respective timing restrictions, such as a long cycle period for update reports, for instance.

4.1.5 Define and perform risk treatment activities

Cybersecurity risks are challenging the risk management and control, as sudden and frequent changes may occur. Therefore, cybersecurity risk management needs to identify relevant changes and monitor them accordingly.

4.1.6 Monitor risks

Monitoring of risks should include:

- Continuous monitoring of new threats and attack paths.
- Continuous monitoring of changes in the attack paths – e.g., by published attacks proving the feasibility has been increased since the last risk analysis.
- Continuous monitoring of accepted risks (Cybersecurity claims), also to provide implicit verification of unmitigated risks.
- Revalidation based on an analysis for integration of an off-the-shelf component (e.g., free and open source software).
- Identification of changes to assumptions and constraints considered for the analysis and evaluation of cybersecurity risks.

- Identification of risks that refer to obsolete techniques, values, items, and assets.
- Changed conditions and results in project implementation, concept, verification, and validation.
- Changed conditions and results of relevant interfaces, such as on transferred risks.

An active exchange with the Automotive Cybersecurity Management System, e.g., on intelligence data as described in aspects e–h of subchapter 4.1.3, may provide further evidence for the effectiveness of monitoring.

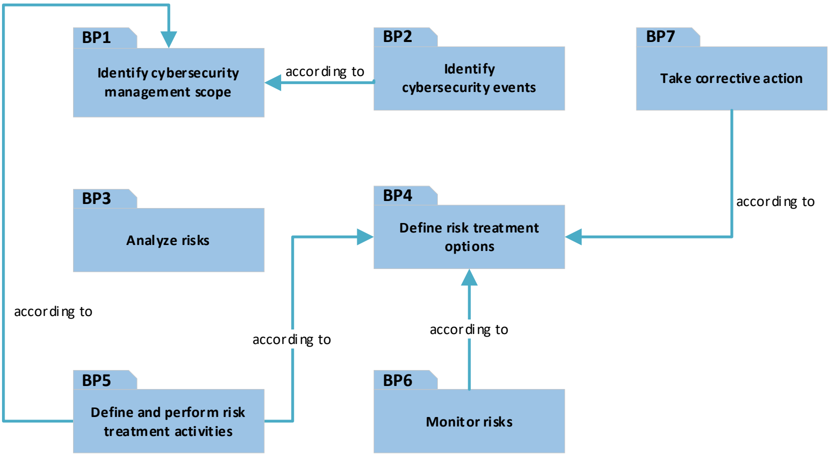
Corrective actions shall be taken appropriately to keep cybersecurity risk evaluation and treatment up to date.

Rating Rules:

> **[MAN.7.RL.6]** If monitoring does not assess fulfillment of activities, the indicator BP6 shall not be rated higher than L.

4.2 Rating rules within the process

The following figure shows the relationships between MAN.7 base practices:


BP1
Identify cybersecurity management scope
BP2
Identify cybersecurity events
BP7
Take corrective action
BP3
Analyze risks
BP4
Define risk treatment options
BP5
Define and perform risk treatment activities
BP6
Monitor risks
according to
according to
according to
according to
according to

These relationships are used as the basis for the rating rules defined in the following subchapters.

BP1: Determine cybersecurity risk management scope.

> **[MAN.7.RL.7]** If the determination of the cybersecurity risk management scope (BP1) is downrated, then the indicator BP2 and BP5 shall be downrated as well.

BP4: Define risk treatment options.

> **[MAN.7.RL.8]** If the definition of risk treatment options is downrated (BP4), the indicators BP5, BP6 and BP7 shall be downrated, respectively.

4.3 Rating rules with other processes at level 1

None.

5 SEC.1 Cybersecurity Requirements Elicitation

The purpose is to specify cybersecurity goals and requirements from the outcomes of cybersecurity risk management and ensure consistency between the threat scenarios, cybersecurity goals and cybersecurity requirements.

The Cybersecurity Requirements Elicitation Process uses the risks where risk treatment involves risk mitigation from the Cybersecurity Risk Management Process (MAN.7) as an input. Such risks are related to a threat scenario. Cybersecurity goals ensure the achievement of an acceptable residual risk. To achieve a cybersecurity goal, a set of functional and/or non-functional cybersecurity requirements will be specified.

Cybersecurity requirements are typically detailed in an iterative process. The justification for the selected risk treatment action is typically documented in the risk measure (OII 08-55).

Cybersecurity claims are, by nature, not subject to risk treatment. The related risk value has been evaluated as a residual risk that is acceptable. Cybersecurity claims maybe reevaluated when new vulnerabilities are identified, or an attack path’s feasibility increases.

Cybersecurity goals and stakeholder requirements can contradict each other, such as when a technical solution for a connected service imposes a high risk of a threat scenario. In these cases, cybersecurity requirements will be derived as a trade-off between said stakeholder requirements and cybersecurity goals in dialog with the customer.

The definition of cybersecurity goals is not limited to the development of a product. Where appropriate, they shall be defined also for post-development phases, such as production and decommissioning.

Vulnerabilities that are discovered during implementation, verification, and validation will change the risk value for particular threat scenarios and require an iteration of the Cybersecurity Requirements Elicitation Process.

5.1 General information

5.1.1 Cybersecurity goals

Cybersecurity goals are top-level requirements that consistently address threat scenarios. Their achievement will be validated in the integrated system.

5.1.2 Cybersecurity requirements

Cybersecurity requirements are particularly desired characteristics of a system, software or hardware. They are consistent with the cybersecurity goal they are derived from. Their implementation will be verified in the corresponding integration level.

Cybersecurity requirements may address, among others:

- Functions that are implemented in mechanics, hardware or software, or cover a combination of these elements.
- Processing of signals from other systems
- Non-functional requirements

5.2 Rating rules within the process

None.

5.3 Rating rules with other processes at level 1

None.

6 SEC.2 Cybersecurity Implementation

The purpose is to refine design of the system, software, and hardware, consistent with the cybersecurity requirements and ensure they are implemented.

The Cybersecurity Implementation Process uses the initial product architecture to perform refinements to the architectural elements and their interfaces based on the cybersecurity goals and requirements. The PAM uses no specific term for an architecture that is related solely to cybersecurity.

Cybersecurity is a property of a product; therefore, the system, software and hardware architecture shall reflect the cybersecurity requirements. This can be achieved by additional elements of the architecture or adaptations to the interfaces between the elements.

The cybersecurity requirements are allocated to one or more elements of the product architecture.

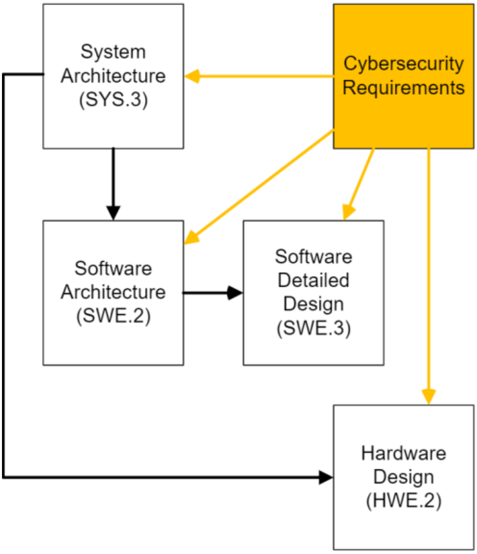

System Architecture (SYS.3)
Cybersecurity Requirements
Software Architecture (SWE.2)
Software Detailed Design (SWE.3)
Hardware Design (HWE.2)

Figure 4 — Allocation of cybersecurity requirements to elements of the product architecture

Cybersecurity controls are used to achieve the cybersecurity goals and cybersecurity requirements. These controls may be complex software algorithms, electronic hardware solutions, or even warnings in a manual for decommissioning. They should be appropriate to mitigate the risk of a threat scenario.

The selection of cybersecurity controls typically has an influence on the system, software, mechanical, and hardware architecture.

Where changes to the elements of the product architecture are necessary the detailed design of such elements will be changed accordingly.

The development of software units as well as the establishing of traceability and consistency is similar to SWE.3.

Vulnerabilities that are discovered during implementation, verification, and validation will change the risk value for particular threat scenarios and require an iteration of the Cybersecurity Requirements Elicitation Process.

6.1 General information

6.1.1 Cybersecurity controls

Typically, cybersecurity controls are technical or other solutions to avoid, detect, counteract or minimize cybersecurity risks. Examples for such measures are:

- Robust software design
- Specific hardware
- Isolation between hardware and software
- Common state-of-the-art solutions
- Encryption

6.1.2 Analyze architecture

The analysis of the system and software architecture in this process is focused on detecting new vulnerabilities. These vulnerabilities are documented so they can be used in risk assessment for the determination of new or updated risk treatment decisions.

Rating Rules:

> **[SEC.2.RL.1]** If no vulnerabilities are found and the analysis is documented, the indicator BP4 must not be downrated.

6.1.3 Appropriate modeling and programming languages

Appropriate modeling and programming languages shall be chosen, based on defined criteria.

Criteria for appropriate modeling and programming languages for cybersecurity can include the use of language subsets, enforcement of strong typing and/or the use of defensive implementation techniques.

Example to cover the defined criteria above could be the use of a coding guideline or an appropriate development environment.

6.2 Rating rules within the process

None.

6.3 Rating rules with other processes at level 1

None.

7 SEC.3 Risk Treatment Verification

The purpose of the Risk Treatment Verification Process 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.

The Risk Treatment Verification Process ensures the implementation of the cybersecurity controls according to the cybersecurity requirements, the corresponding architectural design, and the detailed design.

Cybersecurity controls are in most cases specified by functional or non-functional requirements and a corresponding architectural design and detailed design. They are identified solutions to achieve the cybersecurity requirements.

The objective of the Risk Treatment Verification Process is to prove that the implementation meets these requirements and the specified design. It provides evidence that measures are being done correctly.

In that sense, the verification process cannot measure whether the right measures have been specified and implemented. It cannot provide any evidence of the suitability of a corresponding cybersecurity goal to reduce an associated risk, which is instead in scope of SEC.4.

7.1 General Information

7.1.1 Risk treatment verification measures definition

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

Cybersecurity verification may include, among others:

- Static software analysis
- Software unit testing

- Software integration and acceptance testing
- System integration and acceptance testing

Rating rules:

[SEC.3.RL.1] If the risk treatment verification measures are not based on cybersecurity requirements, architectural design, and the detailed design, then BP1 must not be rated higher than P.

[SEC.3.RL.2] If entry/exit criteria are reasonable specified for a set of verification measures instead of each verification measures, then BP1 shall not be downrated.

7.1.2 Automation of risk treatment verification measures

Rating rules:

[SEC.3.RL.3] If a risk treatment verification measure is automated and the correctness, completeness and consistency of the corresponding scripts and programs are not addressed in the verification measure definition, then BP1 shall be downrated.

7.1.3 Explorative testing and traceability

The state-of-the-art testing not only comprises testing derived from requirements but also explorative testing based on experience, such as "error guessing based on knowledge". This is valuable as it adds to the quality of the product. Therefore, explorative tests that are based on experience cannot, by definition, be traced with the cybersecurity requirements.

Still, traceability is needed between the explorative test cases and their results.

Rating rules:

[SEC.3.RL.4] If risk treatment verification measures representing explorative tests, which, by definition cannot be traced to the cybersecurity requirements, have no such traceability, then BP4 shall not be downrated.

8 SEC.4 Risk Treatment Validation

The purpose of the Risk Treatment Validation Process is to confirm that the integrated system achieves the associated cybersecurity goals.

Cybersecurity goals are high-level requirements addressing an associated threat scenario. To achieve a cybersecurity goal, a set of functional and/or non-functional cybersecurity requirements and a corresponding design are specified. The verification of the implementation against these requirements and the design is in scope of the Risk Treatment Verification Process (SEC.3).

The scope of the Risk Treatment Validation Process is to provide evidence that the right measures have been specified. Thereby, the process SEC.4 probes and questions the defined cybersecurity goals and the associated proposed solutions themselves.

A typical way of validating cybersecurity goals and associated cybersecurity controls is to perform penetration tests that attempt to compromise the system.

Therefore, the risk treatment validation measures shall include validation activities based on effective methods to detect vulnerabilities not identified by the TARA and thus not addressed by specific risk treatment actions.

Validation activities may include validation measures with specified test cases and/or also explorative validation methods with the intent to identify unknown vulnerabilities and attack paths.

Vulnerabilities discovered during validation may affect the risk value for particular threat scenarios and require an iteration of the Cybersecurity Risk Management Process (MAN.7) and Cybersecurity Requirement Elicitation Process (SEC.1); hence a specific handling of the validation results is necessary. This is typically addressed by the Problem Resolution Management Process (SUP.9).

8.1 General Information

8.1.1 Risk treatment validation measures definition

The validation of cybersecurity goals and associated controls includes activities to detect vulnerabilities and unidentified attack paths.

Cybersecurity validation measures may follow the techniques, among others:

- Vulnerability scanning
- Penetration testing
- Fuzz testing

Validation measures may also include inspections, including an analysis of applications and operating systems for security flaws. An inspection can also be done via code reviews.

Rating Rules:

> **[SEC.4.RL.1]** If the risk treatment validation measures are not based on the cybersecurity goals, the indicator BP1 shall not be rated higher than P.
>
> **[SEC.4.RL.2]** If entry/exit criteria are reasonable specified for a set of validation measures instead of each validation measures, then BP1 shall not be downrated.

8.1.2 Automation of risk treatment validation measures

Rating rules:

> **[SEC.4.RL.3]** If a risk treatment validation measure is automated and the correctness, completeness and consistency of the corresponding scripts and programs are not addressed in the validation measure definition, then BP1 shall be downrated.

8.1.3 Perform risk treatment validation activities

In order to check the completeness and appropriateness of the validation activities with respect to the specified risk treatment validation measures, documentation is essential.

Note: This should not be confused with the validation results made available after performing the tests.

Rating Rules:

> **[SEC.4.RL.4]** If documentation of the validation activities is missing or not suitable to evaluate the completeness of the activities according to the specified validation measures, then BP3 shall not be rated higher than P.

Annex A Process Assessment and Reference Model Conformity

A.1 Introduction

The Automotive SPICE process assessment and reference model meet the requirements for conformity defined in ISO/IEC 33004:2015. The process assessment model can be used in the performance of assessments that meet the requirements of ISO/IEC 33002:2015.

This clause serves as the statement of conformity of the process assessment and reference models to the requirements defined in ISO/IEC 33004:2015.

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

Due to copyright reasons each requirement is only referred to by its number. The full text of the requirements can be drawn from ISO/IEC 33004:2015.

A.2 Conformity to the requirements for process reference models

Clause 5.3: "Requirements for process reference models"

The following information is provided in Chapter 1 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 use, and
- 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 that meet the requirements of ISO/IEC 33004:2015 clause 5.4 are provided in Chapter 2 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 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.

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

Clause 5.4: “Process descriptions”

These requirements are met by the process descriptions in Chapter 2 of this document.

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

A.3 Conformity to the requirements for process assessment models

Clause 6.1: "Introduction"

The purpose of this process assessment model is to support assessment of process capability within the automotive domain using the process measurement framework defined in ISO/IEC 33020:2019.

> *[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 subchapter 1.1 of this document. The Automotive SPICE Process Reference Model satisfies the requirements of ISO/IEC 33004:2015, clause 5 as described in Annex A.2.

The process capability scope of this process assessment model is defined in the process measurement framework specified in ISO/IEC 33020:2019, which defines a process measurement framework for process capability satisfying the requirements of ISO/IEC 33003.

> *[ISO/IEC 33004:2015, 6.2]*

Clause 6.3: "Requirements for process assessment models"

The Automotive SPICE Process Assessment Model is related to process capability.

> *[ISO/IEC 33004:2015, 6.3.1]*

This process assessment model incorporates the process measurement framework specified in ISO/IEC 33020:2015, which satisfies the requirements of ISO/IEC 33003.

> *[ISO/IEC 33004:2015, 6.3.2]*

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

This process assessment model is based on the measurement framework defined in ISO/IEC 33020:2015.

> *[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 from ISO/IEC 33020:2015 are addressed.

> *[ISO/IEC 33004:2015, 6.3.5]*

This process assessment model defines

- the selected process quality characteristic,
- the selected process measurement framework,
- the selected process reference model(s), and
- the selected processes from the process reference model(s)

in Chapter 3 of this document.

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

In the capability dimension, this process assessment model addresses all of the process attributes and capability levels defined in the process measurement framework in ISO/IEC 33020:2015.

> *[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 33004:2015, the text of the clause heading is additionally specified for the following three requirements.

The Automotive SPICE 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 subchapter 3.3. The assessment indicators used are:

- Base practices and information items

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

- Generic practices and information items

> *[ISO/IEC 33004:2015, 6.3.1 b: "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 each description of the base practices in Chapter 2.

The mapping of the assessment indicators to the process attributes in the process measurement framework including all of the process attribute achievements is included in each description of the generic practices in Chapter 5 of Automotive SPICE® 4.0.

Each mapping is indicated by a reference in square brackets.

> *[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 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, as it would be found appropriate in 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 stakeholder and contacts - 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
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

ID	Name	Characteristics
		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 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.

ID	Name	Characteristics
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: - 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

ID	Name	Characteristics
		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

ID	Name	Characteristics
		- 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 floorplan and the overall hardware structure • Identifies the required hardware components • Includes the rationale for chosen options of hardware architecture • Identifies own developed and supplied hardware components • Identifies the required internal and external hardware component interfaces • Specifies the interfaces of the hardware components • Specifies the dynamic behavior • Identifies the relationship and dependency between hardware components • Describes all hardware variants to be developed • Describes power supply, thermal and

ID	Name	Characteristics
		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 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
08-57	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

ID	Name	Characteristics
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
12-01	Request for quotation	• Reference to the requirements specifications • Identifies supplier selection criteria • Cybersecurity responsibilities of the supplier • The scope of work regarding cybersecurity, including the cybersecurity goals or the set of

ID	Name	Characteristics
		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
13-22	Traceability record	• All requirements (customer and internal) are to be traced • Identifies a mapping of requirement to life cycle work products • Provides the linkage of requirements to work product decomposition (i.e., requirement, design, coding, testing, deliverables, etc.) • Provides forward and backwards mapping of requirements to associated work products throughout all phases of the life cycle - Note: this may be included as a function of another defined work product (Example: A CASE tool for design decomposition may have a mapping ability as part of its features)
13-24	Validation results	• Validation data, logs, feedback, or documentation • Validation measure passed • Validation measure not passed • Validation measure not executed, and a rationale

ID	Name	Characteristics
		• 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 - 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.
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
14-02	Corrective action	• Identifies the initial problem

ID	Name	Characteristics
		• 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 probability - 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 • 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

ID	Name	Characteristics
		- 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
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

ID	Name	Characteristics
		- 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 required to protect cybersecurity - Associated to one or more threat scenarios
17-52	Cybersecurity controls	• Technical solutions to prevent, detect, or mitigate cybersecurity risks • Associated to one or more cybersecurity requirements
15-55	Cybersecurity threat scenario	• Description how threats exploit a vulnerability or multiple vulnerabilities exposing assets to harm, enabling the corresponding risk

ID	Name	Characteristics
		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 event • 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 parameter containing data applied to the system or software functions, behavior or properties. The notion of application parameter is expressed in two ways: firstly, the logical specification (including name, description, unit, value domain or threshold values or characteristic curves, respectively) and secondly, the actual quantitative data value it receives by means of data application.
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 goal	ISO/SAE 21434	Concept-level cybersecurity requirement associated with one or more threat scenarios.
Cybersecurity property	ISO/SAE 21434	Attribute that can be worth protecting.
Damage scenario	ISO/SAE 21434	Adverse consequence involving a vehicle or vehicle function and affecting a road user
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.
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	**R**e**c**ommendation
RL	**R**u**l**e
ROM	**R**ead **O**nly **M**emory
SPICE	**S**oftware **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
- test cases and verification results.

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

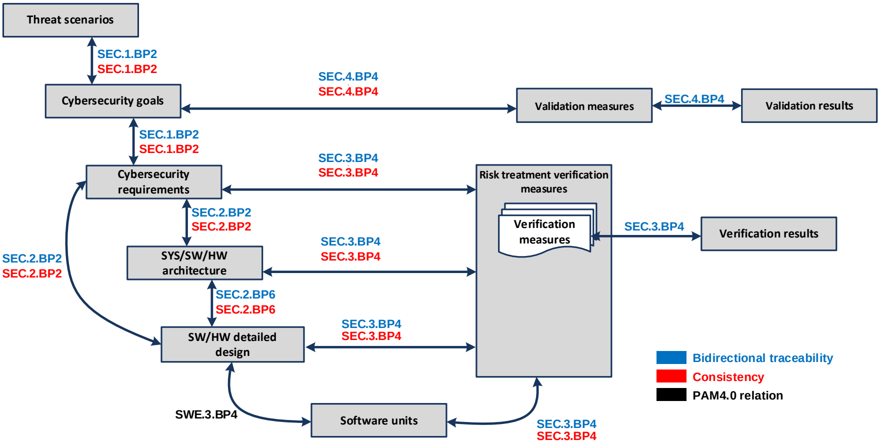


Figure 5 — Bidirectional Traceability and Consistency

Quality Management in the Automotive Industry

You can find the current status of the published VDA volumes on Quality Management in the Automotive Industry (QAI) on the Internet at http://www.vda-qmc.de.

You can also place direct orders at this homepage.

Reference:

Verband der Automobilindustrie e.V. (VDA)
Qualitäts Management Center (QMC)
10117 Berlin, Behrenstr. 35
Phone: +49 (0) 30 89 78 42-235 ; Fax : +49 (0) 30 89 78 42-605
Email: info@vda-qmc.de; Internet: www.vda-qmc.de

VDA QMC

Verband der Automobilindustrie
Qualitäts-Management-Center