VDA QMC

AUTOMOTIVE SPICE®

Automotive SPICE®

Process Reference and Assessment Model for Cybersecurity Engineering

Version 2.0

Automotive SPICE®

网络安全工程过程参考和评估模型

第 2.0 版

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

标题:	Automotive SPICE® 网络安全过程参考和评估模型
作者:	VDA 第 13 工作组
版本:	2.0
日期:	2025-03-28
状态:	已发布

关于翻译

本文为 Automotive SPICE® 网络安全过程参考和评估模型的中文翻译版，是为了帮助读者更好理解英语版原文内容。本文仅限于参考，如果存在对中文翻译内容的疑问，须确认 Automotive SPICE® – VDA QMC (vda-qmc.de)所提供的英语版原文内容。

本文的中文翻译是由以下公司提供支持实施。

悠牧矻信息科技（上海）有限公司

中国（上海）自由贸易试验区芳春路 400 号 1 幢 3 层

consulting@umovcom.com

中文翻译的独立评审由 VDA-QMC 中国软件顾问委员会提供支持实施。

VDA QMC
德国汽车工业协会
质量管理中心中国分公司
CHINA

VDA QMC
SWQ AB China
Software Quality
Advisory Board China

VDA-QMC 中国软件质量顾问委员会

swq.abc@vdachina.com.cn

Copyright notice

Acknowledgement

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

Derivative works

Document distribution

Change requests

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

Trademark notice

Document history

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

版权声明

致谢

VDA、VDA QMC 及第 13 工作组诚挚感谢 intacs®工作组成员的高质量工作。我们感谢所有参与 Automotive SPICE®制订和发布的人员。

衍生著作

文档分发

变更请求

任何问题或变更请求需要通过 www.vda-qmc.de 网站所定义的机制进行报告。

商标声明

文档历史

版本	日期	作者	记录
1.0	2021-07-16	VDA QMC PG13	初版
2.0	**2025-03-28**	**VDA QMC WG13**	**CS PAM 修订，以适配 4.0**

Table of contents

目录

List of Figures

List of Tables

图录

表录

1. Introduction

1.1. Scope

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

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

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

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

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

1.2. Relation to ISO/SAE 21434

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

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

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

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

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

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

1. 介绍

1.1. 范围

联合国欧洲经济委员会 UNECE 法规中的 R155 法规要求汽车制造商需识别和管理供应链中的网络安全风险。Automotive SPICE 是一个过程评估模型，当它与适当的评估方法一起使用时，有助于识别过程相关的产品风险。为了将网络安全相关过程纳入已被证明的 Automotive SPICE 范围内，在网络安全工程的过程参考及评估模型（网络安全 PAM）中定义了额外的过程。

本文档对 Automotive SPICE® 4.0 进行了补充，使其能够对网络安全相关的开发过程进行评估。

使用 Automotive SPICE® 网络安全 PAM 进行评估的前提条件是，基于推荐的 VDA 评估范围的 Automotive SPICE 的评估结果已经存在。否则， 需要同时使用 Automotive SPICE ® 网络安全 PAM 和包含推荐的 VDA 评估范围过程的 Automotive SPICE ® PAM 进行评估。

附录 B 包含了与 Automotive SPICE®网络安全过程相关的信息项特性子集。

附录 C 包含了与 Automotive SPICE®网络安全过程相关的术语子集。

1.2. 与 ISO/SAE 21434 的关系

Automotive SPICE 评估的目的是识别主要过程、组织过程和支持过程中的系统性弱点。

Automotive SPICE® 网络安全的评估可以识别正在实施网络安全活动的项目中的差距和过程弱点。这些差距和弱点是改进组织内部网络安全过程的宝贵输入。通过实施源自评估结果的有效改进措施，该组织将能够调整和完善网络安全管理体系。

Automotive SPICE® 4.0 和 Automotive SPICE®网络安全覆盖系统工程、软件工程和硬件工程。机械工程的指标不属于当前 Automotive SPICE® PAM 的一部分。

Automotive SPICE 的风险范围有意地超出了 ISO/SAE 21434 所定义的范围。ISO/SAE 21434 聚焦于道路使用者，而 Automotive SPICE® 网络安全则关注整个汽车生态系统中可能对网络安全相关的软件系统开发产生影响的风险。

ISO/SAE 21434 的某些方面不属于本文档的范围，因为它们不在开发项目的背景中执行。这些方面由 ISO PAS 5112 应对，是网络安全管理体系审核的内容。

本文档支持分布式网络安全活动、概念开发、产品开发、网络安全确认、威胁分析和风险评估的过程能力确定。

Project-dependent cybersecurity management is supported as follows:

- Cybersecurity responsibilities:
  GP 2.1.3: Determine resource needs.
- Cybersecurity planning:
  GP 2.1.2 – Plan the performance of the process and
  MAN.3 – Project Management.
- Tailoring of cybersecurity activities:
  PA 3.2 – Process deployment, and
  GP 2.1.2 – Plan the performance of the process.
- Reuse:
  included in make-buy reuse analysis SWE.2.BP3: Analyze software architecture,
  SYS.3.BP3: Analyze system architecture, and
  REU.2 – Management of Products for Reuse.
- Component out of context: covered by Cybersecurity Engineering Process Group (SEC) based on assumptions regarding cybersecurity goals.
- Off-the-shelf component:
  MAN.3.BP7 Define and monitor project interfaces and agreed commitments,
  Automotive SPICE® Guideline v2.0, chapter 2.5.3 Development external to the project, and
  MAN.7 – Cybersecurity Risk Management.
- Cybersecurity case:
  input provided by base practices “summarize and communicate results” of engineering processes.
- Cybersecurity assessment:
  Automotive SPICE® for Cybersecurity is a model for process capability determination. An in-depth technical analysis is not part of an Automotive SPICE® for Cybersecurity assessment.
- Release for post-development:
  SPL.2 – Product Release,
  SUP.8 – Configuration Management, and
  SUP.1 – Quality Assurance.
- Request for quotation:
  ACQ.2 Supplier Request and Selection
- Alignment of responsibilities:
  ACQ.4 Supplier Monitoring

1.3. Requirements on Assessment Scope

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

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

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

Rationale:

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

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

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

对依赖于项目的网络安全管理的支持如下：

- 网络安全职责：
  GP 2.1.3 – 确定资源需要。
- 网络安全规划：
  GP 2.1.2 – 计划过程的实施 和
  MAN.3 –项目管理。
- 网络安全活动裁剪：
  PA 3.2 – 过程部署 和
  GP 2.1.2 – 计划过程的实施。
- 复用:
  包含在 开发-购买-复用分析中，如 SWE.2.BP3: 分析软件架构、
  SYS.3.BP3: 分析系统架构 和
  REU.2 –复用产品管理。
- 独立于环境组件：由网络安全工程过程组（SEC）基于网络安全目标的假设而覆盖。
- 现成组件:
  MAN.3.BP7 定义和监控项目接口和约定的承诺、
  Automotive SPICE® 指南 v2.0, 第 2.5.3 章节 被评估项目外部的开发 和
  MAN.7 – 网络安全风险管理。
- 网络安全档案:
  由工程过程的基本实践“总结和沟通结果”提供输入。
- 网络安全评估:
  Automotive SPICE® 网络安全是一个过程能力确定模型。深入的技术分析并不是 Automotive SPICE® 网络安全评估的内容。
- 开发后发布:
  SPL.2 – 产品发布、
  SUP.8 – 配置管理和
  SUP.1 – 质量保证。
- 报价请求:
  ACQ.2 供应商请求和选择
- 职责的对齐:
  ACQ.4 供应商监控

1.3. 对评估范围的要求

通常，有关范围的决策由评估赞助方自行决定。

当已有评估是覆盖所有的过程域，则不需要针对 SUP 过程组进行重新评估。如果评估是在与网络安全相关的开发环境中进行的，则~~所有~~ PRM 和 PAM 中所有特定于网络安全的方面都必须纳入考虑。

在 Automotive SPICE® 指南 （第二版）的第 10.2 章中，对已有评估的有效性进行了描述。

理由如下:

SEC.4 风险处理确认过程侧重于网络安全目标，而 VAL.1 确认过程涉及所有利益相关方目标或利益相关方需求。

如果将这两个过程的目的进行比较，其差异显而易见。

SEC.4 的目的被阐述为确认集成后的系统达成相关的网络安全目标。

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

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

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

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

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

2. Statement of Compliance

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

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

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

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

而 VAL.1 的目的则是提供证据，来证明交付的产品在其运行目标环境中满足其预期的使用期望。网络安全目标通常来源于损害场景所考虑的安全属性，以及攻击路径分析，并包括非预期使用。这可以在实际环境或模拟环境中进行确认。

风险处理确认过程是证明非预期使用不应导致非期望的产品行为。该确认是确保交付产品的接收方的期望得到满足。

ACQ.2 被描述为对开发网络安全相关产品的供应商进行潜在分析的过程。因此，它应该在这个特定的背景下进行评估。另一方面，Automotive SPICE®潜在分析（PoA）可以在任何情况下使用。

Automotive SPICE®网络安全评估的范围可被适当裁剪。例如，如果供应商不参与网络安全目标的确认，则 SEC.4 可被排除在评估范围之外。

2. 符合性声明

Automotive SPICE 过程评估模型及过程参考模型符 ISO/IEC33004:2015，可作为实施过程能力评估的基础来使用。

Automotive SPICE® 4.0 被用作符合 ISO/IEC 33003:2015 的度量框架。

附录 A 提供了过程评估模型及过程参考模型对于 ISO/IEC 33004:2015 要求的符合性声明。

Automotive SPICE® 4.0 附录 A 提供了度量框架对于 ISO/IEC 33003:2015 要求的符合性声明。

3. Process Capability Determination

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

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

The relationship is shown in Figure 1:

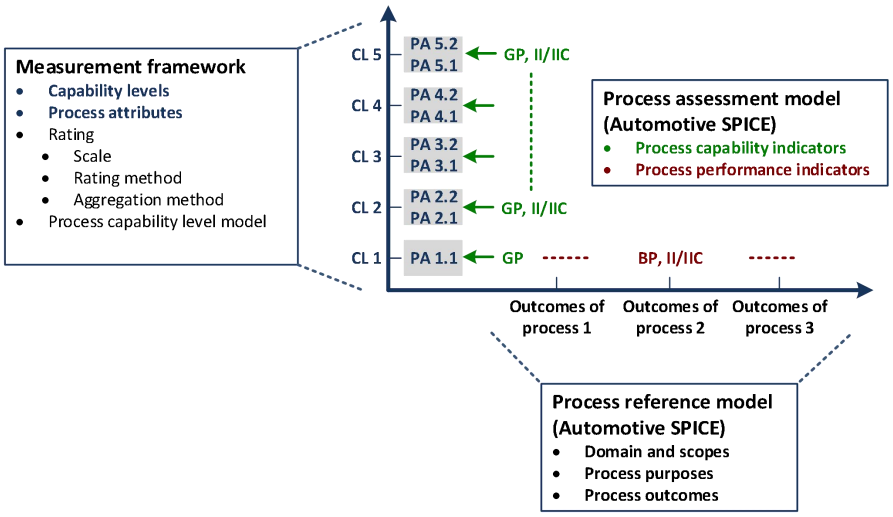

Figure 1— Process Assessment Model Relationship

3.1. Process reference model

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

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

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

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

3. 过程能力确定

使用过程评估模型来确定过程能力的概念是基于一个二维框架。第一个维度是由过程参考模型（过程维度）定义的过程来提供。第二个维度是由进一步细分到过程属性的能力级别（能力维度）所构成。过程属性提供了过程能力可度量的特性。

过程评估模型从过程参考模型中选择过程并增补了指标。这些指标支持收集客观证据，使评估师能够根据能力维度对过程进行评级。

关系如图 1 所示：

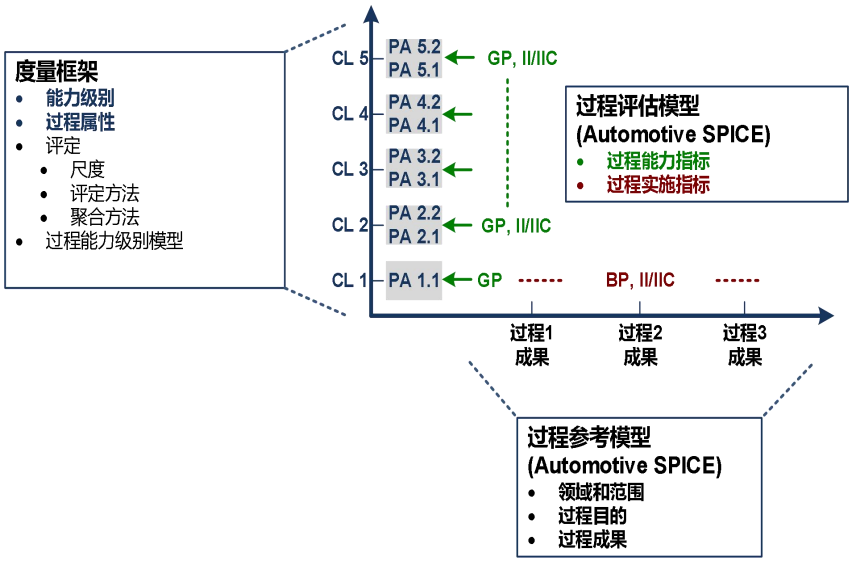

图 1— 过程评估模型关系

3.1. 过程参考模型

所有过程根据其所处理的活动领域被收集至不同的过程组。

这些过程组总共分为三个过程类别：主要过程，组织过程和支持过程。
对于各个过程，都制定了目的陈述，其内容包括在特定环境下执行该过程时的特有功能性目标。针对每个目的陈述，都有一个相关联的特定成果清单，作为过程实施预期的正面结果。

针对过程维度，Automotive SPICE®和 Automotive SPICE®网络安全的过程参考模型提供了过程集合，如图 2 所示。本文档描述与网络安全相关的过程。关于其他过程，参见 Automotive SPICE® 4.0.

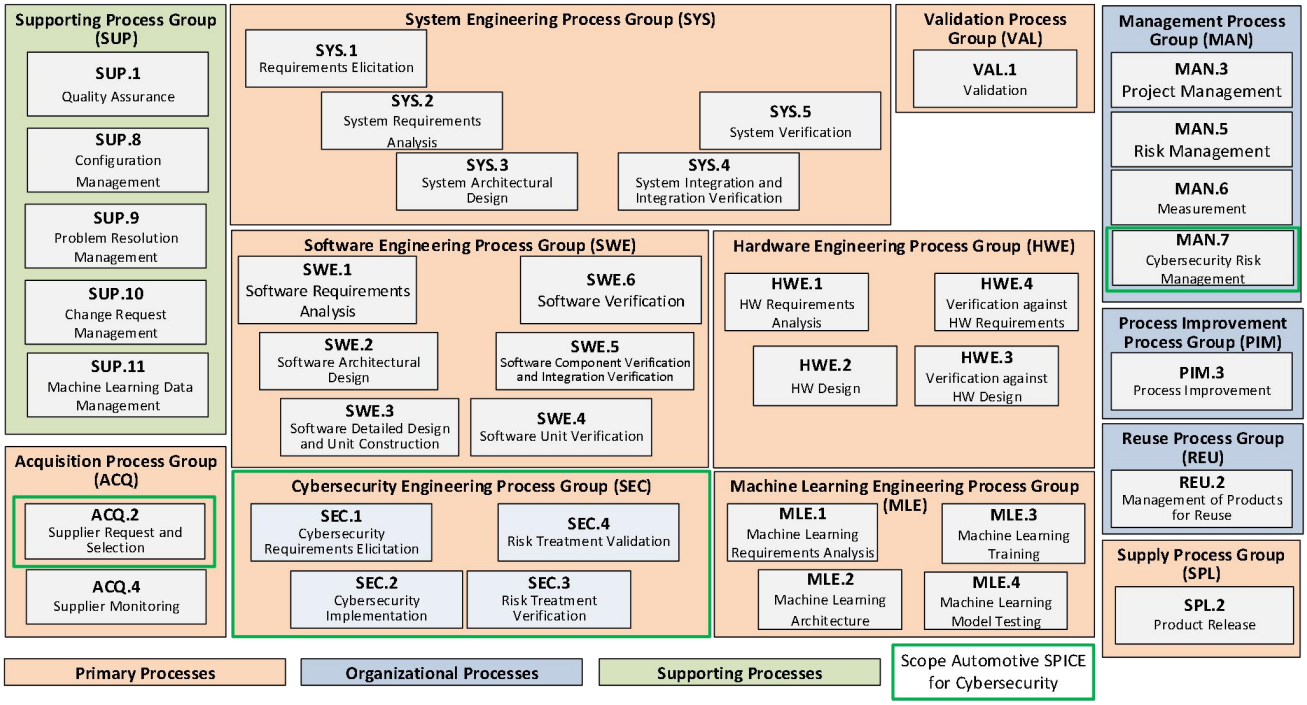

Figure 2— Automotive SPICE® + Cybersecurity Process Reference Model – Overview

3.1.1. Primary Processes category

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

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

- the Acquisition Process Group
- the Cybersecurity Engineering Process Group

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

ACQ.2	Supplier Request and Selection

Table1 — Primary Life Cycle Processes – ACQ

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

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

Table 2— Primary Processes – SEC

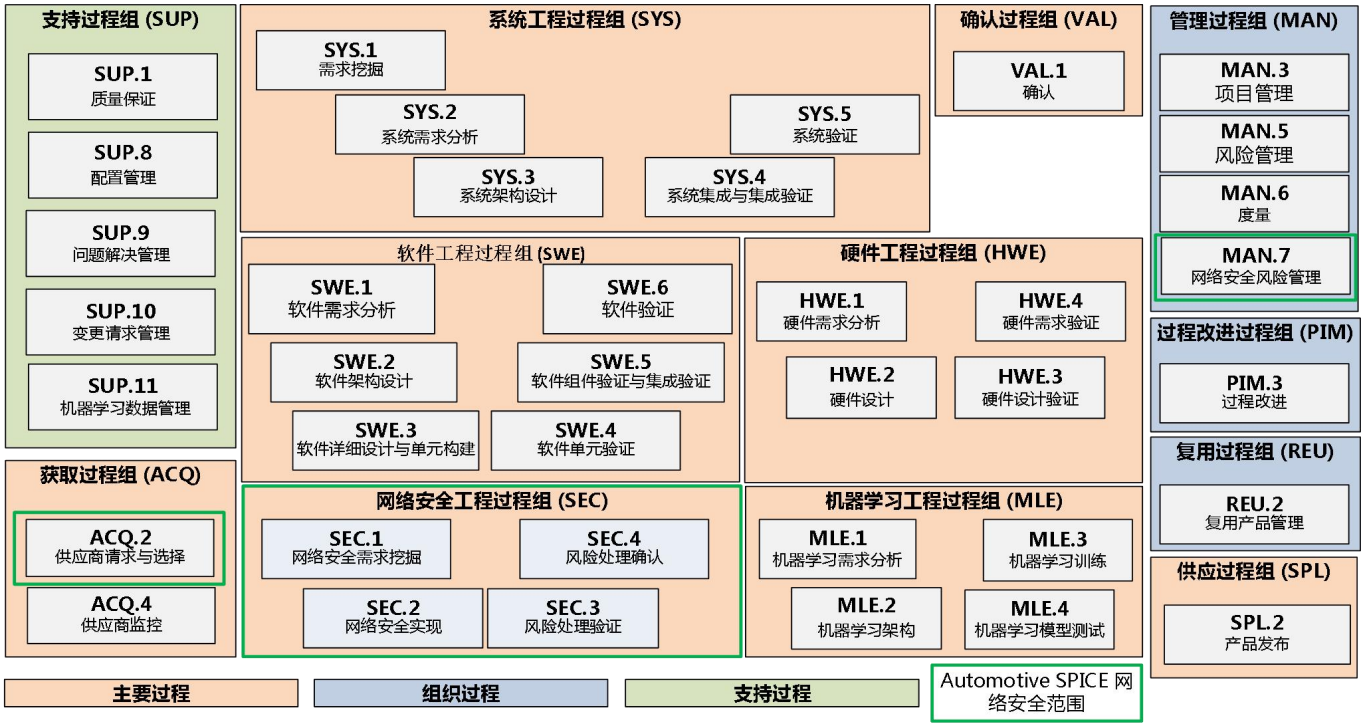

图 2 — Automotive SPICE® + 网络安全过程参考模型 – 概览

3.1.1. 主要过程类别

主要过程类别是由可适用从供应商获取产品的过程，或回应利益相关方需要以及交付产品时可适用于产品开发的过程所组成，包括规范、设计、实现、集成和验证所需的工程过程。

Automotive SPICE®网络安全的主要过程类别包括以下过程组：

- 获取过程组
- 网络安全工程过程组

获取过程组（ACQ）包括客户执行的过程，或者当供应商为了获取产品或服务而作为其供应商的客户时所执行的过程。

ACQ.2	供应商请求和选择

表 1 — 主要生命周期过程 – ACQ

网络安全工程过程组（SEC）包括为了达成网络安全目标所执行的过程。

SEC.1	网络安全需求挖掘
SEC.2	网络安全实现
SEC.3	风险处理验证
SEC.4	风险处理确认

表 2 — 主要过程 – SEC

3.1.2. Organizational Processes category

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

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

- the Management Process Group

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

MAN.7	Cybersecurity Risk Management

Table 3 — Organizational Processes – MAN

3.2. Measurement framework

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

3.3. Understanding the level of abstraction of a PAM

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

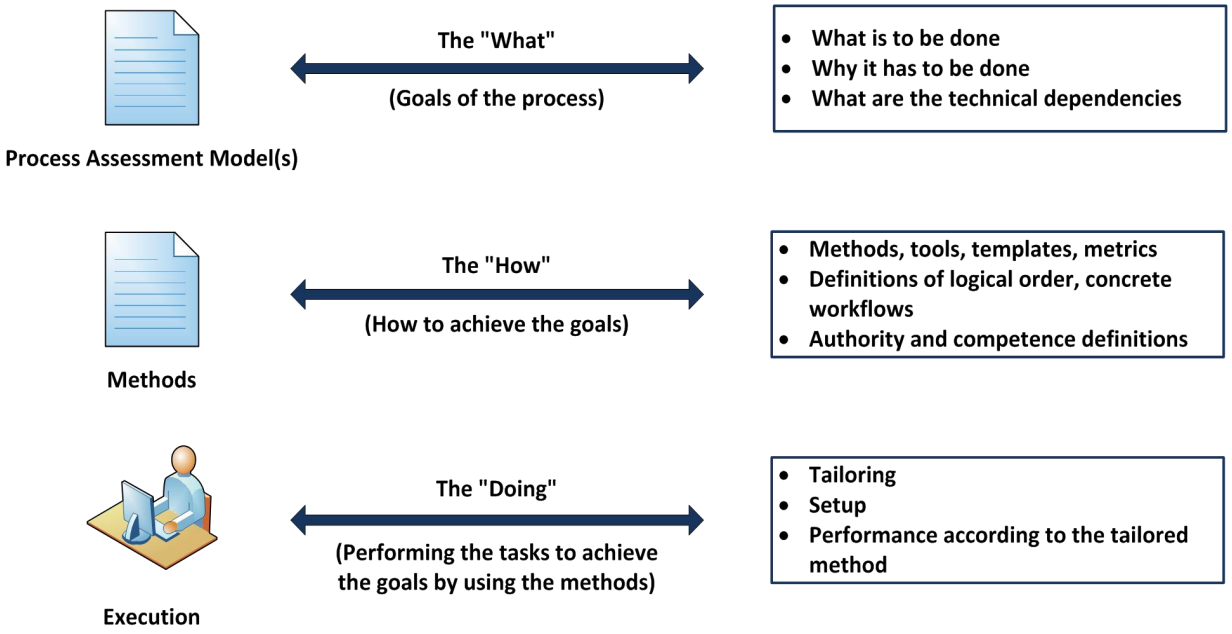

Figure 3— Possible Levels of Abstraction for the Term "Process"

3.1.2. 组织过程类别

组织过程类别是由开发过程、产品以及资源资产的过程所组成。这些过程、产品和资源资产在组织内的项目中使用时，将帮助组织实现其业务目标。

Automotive SPICE®网络安全的组织过程类别包括以下过程组：

- 管理过程组

管理过程组（MAN）是由在生命周期内管理任何类型的项目或过程的任何人可使用的过程所组成。

MAN.7	网络安全风险管理

表 3— 组织过程 – MAN

3.2. 度量框架

过程能力级别、过程属性、评定尺度和能力级别评定模型与 Automotive SPICE® 4.0.中的定义相一致。

3.3. 理解 PAM 的抽象级别

"过程（process）" 这一术语可以从三个抽象层级来理解。需要注意的是，这些抽象层级并不是用来做严格的非黑即白的划分，也不是为了提供一种科学的分类模式。这里要传达的信息是，要理解在实践中，"过程（process）" 这一术语具有不同的抽象层级，而 PAM 处于最高层。

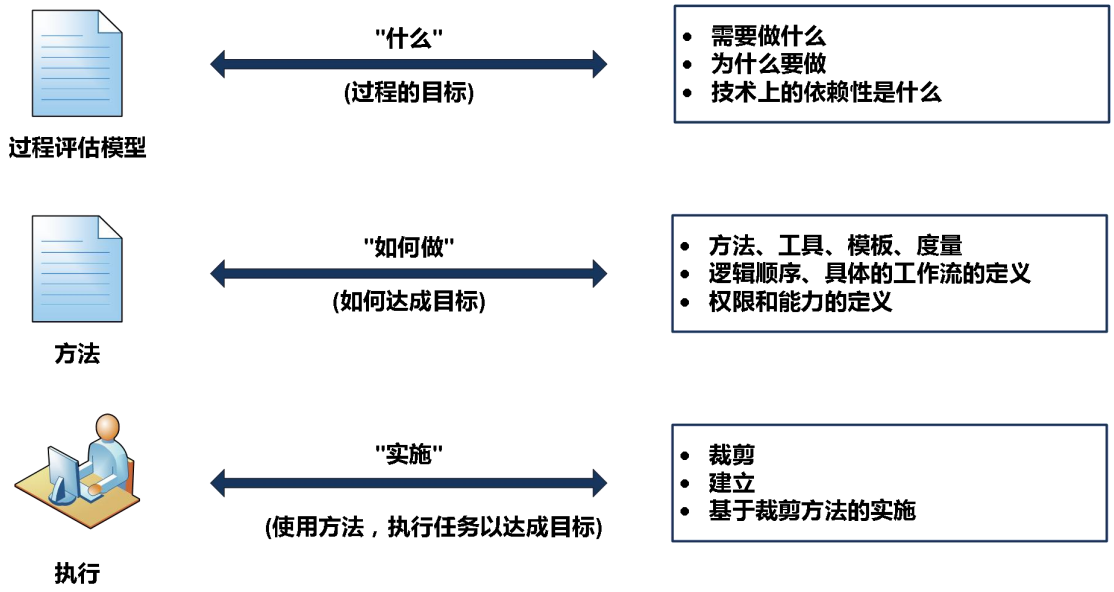

图 3— 关于术语“过程”的可能的抽象层面

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

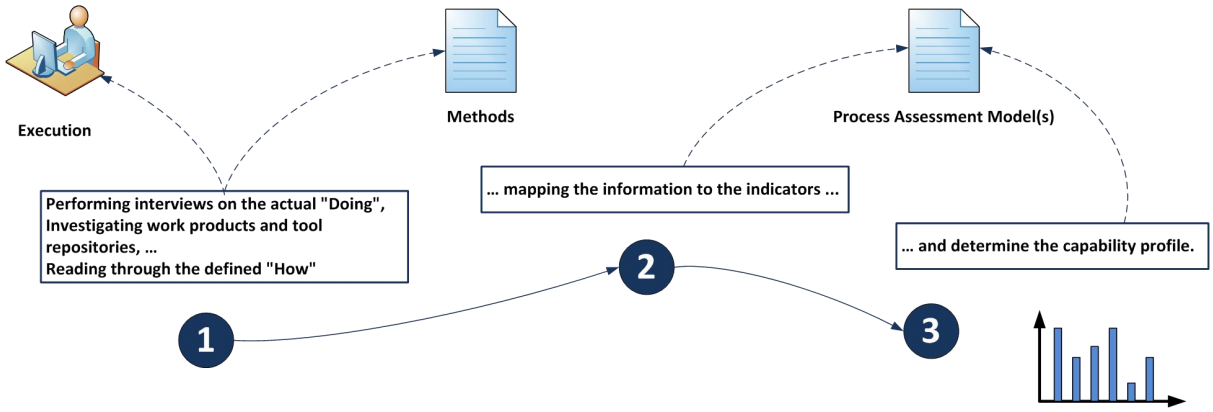

Figure 4— Performing a Process Assessment for Determining Process Capability

收集在产品开发过程中获得的经验（即在“实施”层级），若与他人分享，则意味着需要创建一个“如何做”层级。然而，“如何做”总是特定于某一特定的环境，例如某家公司、某个组织单位或者某个产品线。举例而言，项目、组织单位，或公司 A 的“如何做”可能并不能直接适用于项目、组织单位或公司 B。然而，两者都被希望符合过程成果和过程属性达成的 PAM 指标所代表的原则。这些指标位于”什么”的层级，而至于具体模板、规程、工具等该如何解决的决定则属于“如何做”层级。

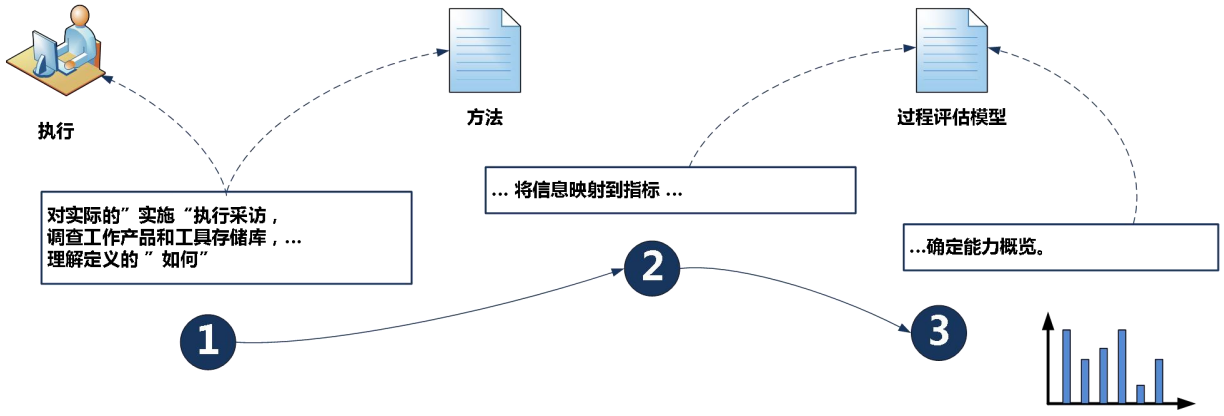

图 4— 执行确定过程能力的过程评估

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

4.1. Acquisition Process Group (ACQ)

4.1.1. ACQ.2 Supplier Request and Selection

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

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

4. 过程参考模型和实施指标（能力等级 1 级）

4.1. 获取过程组（ACQ）

4.1.1. ACQ.2 供应商请求和选择

过程 ID
ACQ.2
过程名称
供应商请求和选择
过程目的
其目的是：基于相关准则选择一个供应商，以达成承诺/协议。
过程成果
1) 建立了供应商评估准则。 2) 根据定义的准则，评估了供应商。 3) 向候选供应商发出了报价请求。 4) 约定了承诺/协议及纠正措施。基于评估结果的考量，与供应商签订了合同。

基本实践
ACQ.2.BP1：建立供应商评估准则。分析相关要求，定义供应商能力评估准则。 *注 1：评估准则的定义可考虑：* • *功能和非功能需求* • *供应商网络安全能力的技术评估，包括网络安全概念和方法（威胁分析和风险评估、攻击模型、漏洞分析等）* • *供应商组织在网络安全方面的能力（例如：在开发中、适用的开发后活动（如生产、运营和报废）、治理、质量和信息安全方面的网络安全最佳实践）* • *持续运营，包括网络安全* • *通过在以前的项目中对供应商的监控，获得了供应商在网络安全方面能力和表现的证明。*
ACQ.2.BP2：评估潜在供应商。收集关于供应商能力的信息，并根据建立的评估准则进行评估。列出首选供应商的名单，并记录结果。 *注 2: 以下方式可支持对潜在供应商的评估：* • *之前 Automotive SPICE® 网络安全评估的摘要* • *组织网络安全管理系统的证据（例如：组织审核的结果，如存在）* • *信息安全管理系统的证据* • *组织的质量管理体系适合/能够支持网络安全工程的证据* • 先前获取的经验

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

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

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

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

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

ACQ.2.BP3：准备并发出报价请求。根据评估识别候选供应商。准备并发出报价请求，包括对已识别偏差的纠正措施计划。

ACQ.2.BP4：协商并授予承诺/协议。根据对报价请求回复的评估，建立一份承诺/协议，包括相关要求和约定的纠正措施。

注 3: 分布式网络安全活动可在一份网络安全接口协议中规定，应考虑所有相关方面 (例如：联络人、裁剪、责任、信息共享、里程碑、时间安排)。

注 4：如果交付物没有包含任何支持（例如：自由和开源软件），则不需要接口协议。

ACQ.2 供应商请求和选择	成果 1	成果 2	成果 3	成果 4
输出信息项				
02-01 承诺/协议				X
02-50 接口协议				X
08-55 风险处理				X
12-01 报价请求			X	
14-02 纠正措施			X	X
15-21 供应商评估		X		
18-50 供应商评估准则	X	X		
基本实践				
BP1：建立供应商评估准则	X			
BP2：评估潜在供应商		X		
BP3：准备并发出报价请求			X	X
BP4：协商并授予承诺/协议				X

4.2. Management Process Group (MAN)

4.2.1. MAN.7 Cybersecurity Risk Management

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

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

4.2. 管理过程组（MAN）

4.2.1. MAN.7 网络安全风险管理

过程 ID
MAN.7
过程名称
网络安全风险管理
过程目的
其目的是：定期识别、分析、按优先级排序并监控对有关利益相关方产生损害的风险。
过程成果
1) 定义了相关项，包括相关项的功能和边界。 2) 识别并定期更新了相关资产、威胁和损害场景。 3) 根据影响评级和攻击可行性评级，分析了网络安全风险，以支持风险处理的优先级排序。 4) 确定了风险状态和风险处理活动的进展 5) 根据风险的优先级、可能性和后果或者其他定义的风险阈值，采取了适当的处理以缓解风险的影响。

Base Practices
MAN.7.BP1：识别网络安全风险管理范围。识别并定期更新网络安全风险管理范围，包括相关项、相关项的功能及其与受影响方的边界。 *注 1：风险可包括技术风险、经济风险和进度风险。* *注 2：风险可包括供应商的交付物和服务。* *注 3：风险源在整个产品生命周期可发生变化。*
MAN.7.BP2：识别网络安全事件。识别和定期评估网络安全信息，并导出潜在网络安全事件。更新与受影响方相关的资产、损害和威胁场景。
MAN.7.BP3：分析风险。根据潜在网络安全事件可能的影响和攻击路径被利用的可行性，分析并确定潜在网络安全事件的风险，以支持风险处理的优先级排序。 *注 4：可以使用不同的方法来分析系统的技术风险，例如：TARA 包括攻击路径分析、仿真、ETA、ATA、FTA 等。*
MAN.7.BP4：定义风险处理方案。针对每个风险，选择一个处理方案以保留、减少、避免或者转移（分担）风险。

MAN.7.BP5: Define and perform risk treatment activities. Define and perform risk activities for risk treatment options.

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

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

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

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

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

MAN.7.BP5：定义和执行风险处理活动。定义和执行针对风险处理方案的风险处理活动。

MAN.7.BP6：监控风险。定期重新评估已识别的潜在网络安全事件相关的风险，以确定网络安全风险状态的变化，重新评估风险处理方案，并评审风险处理活动的进展。

注 5：高优先级的风险可能需要传达给更高管理层并由其进行监控。

MAN.7.BP7：采取纠正措施。当风险处理活动不再有效时，采取适当的纠正措施。

注 6：纠正措施可涉及重新评估风险，开发和实施新的缓解概念或者调整现有概念。

MAN.7 网络安全风险管理	成果 1	成果 2	成果 3	成果 4	成果 5
输出信息项					
08-55 风险处理			X	X	X
14-02 纠正措施				X	X
15-09 风险状态				X	X
15-51 分析结果	X	X	X		
17-53 网络安全威胁场景		X			
基本实践					
BP1: 识别网络安全风险管理范围	X	X			
BP2：识别潜在网络安全事件		X			
BP3：分析风险			X		
BP4：定义风险处理方案				X	X
BP5：定义和执行风险处理活动				X	X
BP6：监控风险				X	
BP7：采取纠正措施					X

4.3. Cybersecurity Engineering Process Group (SEC)

4.3.1. SEC.1 Cybersecurity Requirements Elicitation

Process ID
SEC.1
Process name
Cybersecurity Requirements Elicitation
Process purpose
The purpose is to specify cybersecurity goals and requirements from the outcomes of cybersecurity risk management covering the threat scenarios.
Process outcomes
1) Cybersecurity goals are specified. 2) Cybersecurity requirements are derived from cybersecurity goals. 3) Consistency and bidirectional traceability are maintained between cybersecurity requirements and goals and between the cybersecurity goals and the threat scenarios. 4) The cybersecurity requirements are agreed and communicated to all affected parties.

Base practices
SEC.1.BP1: Specify cybersecurity goals and cybersecurity requirements. Specify cybersecurity goals for the threat scenarios according to the decisions regarding risk treatment to achieve risk reduction. Specify functional and non-functional cybersecurity requirements for the cybersecurity goals. Specify these according to defined characteristics for requirements. *Note 1: This includes the refinement of requirements during iterations of this process.* *Note 2: This includes requirements for post-development phases which may include production, operation, maintenance and decommissioning.* *Note 3: Characteristics of requirements are defined in standards such as ISO IEEE 29148, ISO 26262-8:2018, or the INCOSE Guide To Writing Requirements.* *Note 4: Examples for defined characteristics of requirements shared by technical standards are verifiability (i.e., verification criteria being inherent in the requirements text), unambiguity/comprehensibility, freedom from design and implementation, and not contradicting any other requirements.*
SEC.1.BP2: Ensure consistency and establish bidirectional traceability. Ensure consistency and establish bidirectional traceability between the cybersecurity requirements and the cybersecurity goals. Ensure consistency and establish bidirectional traceability between the cybersecurity goals and the threat scenarios.
SEC.1.BP3: Communicate agreed cybersecurity requirements. Communicate agreed cybersecurity requirements to all affected parties. *Note 5: Cybersecurity goals might be communicated as well to provide additional context information for the derived cybersecurity requirements.*

4.3. 网络安全工程过程组（SEC）

4.3.1. SEC.1 网络安全需求挖掘

过程 ID
SEC.1
过程名称
网络安全需求挖掘
过程目的
其目的是：依据覆盖威胁场景的网络安全风险管理成果，定义网络安全目标和需求。
过程成果
1) 定义了网络安全目标。 2) 从网络安全目标导出了网络安全需求。 3) 维护了网络安全需求与目标之间，以及网络安全目标与威胁场景之间的一致性和双向可追溯性。 4) 约定了网络安全需求，并与所有受影响方沟通。

基本实践
SEC.1.BP1：定义网络安全目标和网络安全需求。根据风险处理决策，为威胁场景定义网络安全目标，以实现风险降低。 根据定义的需求特性，为网络安全目标定义功能性和非功能性网络安全需求。 *注 1：该实践包括此过程迭代中的需求完善。* *注 2：该实践包括开发后阶段需求，例如生产、运营、维护和报废。* *注 3：需求特性在一些标准中有定义，诸如 ISO IEEE 29148、ISO/IEC IEEE 24765、ISO 26262-8:2018 或 INCOSE 需求编写指南等。* *注 4：上述标准共有的关于已定义的需求特性的示例如，可验证的 (即：需求文本中固有的验证准则)、无歧义的/可理解的、无设计和实现限制的、以及不与任何其他需求相矛盾的。*
SEC.1.BP2：确保一致性和建立双向可追溯性。确保网络安全需求与网络安全目标之间的一致性并建立双向可追溯性。确保网络安全目标与威胁场景之间的一致性并建立双向可追溯性。
SEC.1.BP3：沟通约定的网络安全需求。与所有受影响方沟通约定的网络安全需求。 *注 5：同样也可沟通网络安全目标，为导出的网络安全需求提供附加的背景信息。*

SEC.1 Cybersecurity Requirements Elicitation	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Output Information Items				
17-00 Requirement	X	X		
17-54 Requirement Attribute	X	X		
15-51 Analysis Results	X	X		
13-51 Consistency Evidence			X	
13-52 Communication Evidence				X
17-51 Cybersecurity goals	X			
Base Practices				
BP1: Specify cybersecurity goals and cybersecurity requirements.	X	X		
BP2: Ensure consistency and establish bidirectional traceability			X	
BP3: Communicate agreed cybersecurity requirements				X

4.3.2. SEC.2 Cybersecurity Implementation

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

SEC.1 网络安全需求挖掘	成果 1	成果 2	成果 3	成果 4
输出信息项				
17-00 需求	X	X		
17-54 需求属性	X	X		
15-51 分析结果	X	X		
13-51 一致性证据			X	
13-52 沟通证据				X
17-51 网络安全目标	X			
基本实践				
BP1：定义网络安全目标和网络安全需求	X	X		
BP2：确保一致性和建立双向可追溯性			X	
BP3：沟通约定的网络安全需求				X

4.3.2. SEC.2 网络安全实现

过程 ID
SEC.2
过程名称
网络安全实现
过程目的
其目的是：完善系统、软件和硬件设计，与网络安全需求一致，并确保其得到实现。
过程成果
1) 完善了系统、软件和硬件的架构。 2) 建立了网络安全需求与系统架构、软件架构以及硬件架构组件的一致性和双向可追溯性；建立了网络安全需求与软件详细设计以及硬件详细设计的一致性和双向可追溯性。 3) 选择了适当的网络安全管控。 4) 分析了弱点。 5) 完善了软件和硬件的详细设计。 6) 建立了软件架构与软件详细设计的一致性和双向可追溯性；建立了硬件架构组件和硬件详细设计的一致性和双向可追溯性。 7) 与所有受影响方沟通了约定的网络安全实现。

Base practices
SEC.2.BP1: Refine the details of the architecture. The architecture of the system, software, and hardware is refined based on cybersecurity requirements. *Note 1: Refinement here means to add, adapt, or rework elements of the architectures.*
SEC.2.BP2 Ensure consistency and establish bidirectional traceability for cybersecurity requirements. Ensure consistency and establish bidirectional traceability between cybersecurity requirements and system architecture, software architecture and components of hardware architecture. Ensure consistency and establish bidirectional traceability between cybersecurity requirements and software detailed design and hardware detailed design.
SEC.2.BP3: Select cybersecurity controls. Select appropriate cybersecurity controls to achieve or support the cybersecurity requirements including an explanation of how the related risk is mitigated. *Note 2: Typically, cybersecurity controls are technical measures or other solutions to detect, counteract or mitigate cybersecurity risks.*
SEC.2.BP4: Analyze architecture for weaknesses. Analyze the architecture of the system, software, and hardware, incl. interfaces and detailed design regarding weaknesses to identify vulnerabilities. Document the design decisions.
SEC.2.BP5: Refine the detailed design. The detailed design is refined based on the architecture of the software and hardware. *Note 3: Refinement here means to add, adapt or rework elements of the detailed design.*
SEC.2.BP6: Ensure consistency and establish bidirectional traceability for architecture and detailed design. Ensure consistency and establish bidirectional traceability between the software architecture and software detailed design. Ensure consistency and establish bidirectional traceability between the components of hardware architecture and hardware detailed design.
SEC.2.BP7: Communicate agreed results of cybersecurity implementation. Communicate the agreed results of the cybersecurity implementation to all affected parties. *Note 4: The communicated contents may include both results of the cybersecurity implementation and vulnerabilities identified within the architecture.*

SEC.2 Cybersecurity Implementation	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5	Outcome 6	Outcome 7
Output Information Items							
04-04 Software Architecture	X	X					
04-05 Software Detailed Design		X			X		
04-06 System Architecture	X	X					
04-52 Hardware Architecture	X	X					
04-53 Hardware Detailed Design		X			X		
13-51 Consistency Evidence		X				X	

基本实践
SEC.2.BP1：完善架构的细节。基于网络安全需求，完善系统、软件和硬件架构。 *注 1：“完善”这里是指添加、调整或重构架构要素。*
SEC.2.BP2：为网络安全需求确保一致性和建立双向可追溯性。确保网络安全需求与系统架构、软件架构以及硬件架构组件之间的一致性并建立双向可追溯性。确保网络安全需求与软件详细设计和硬件详细设计之间的一致性并建立双向可追溯性。
SEC.2.BP3：选择网络安全管控。选择适当的网络安全管控以实现或支持网络安全需求，包括对相关风险如何得到缓解的解释。 *注 2：通常，网络安全管控是探测、抵抗或缓解网络安全风险的技术措施或其他解决方案。*
SEC.2.BP4：分析架构弱点。分析系统、软件和硬件架构，包括接口和详细设计的弱点，以识别漏洞。记录设计决策。
SEC.2.BP5：完善详细设计。基于软件和硬件架构，完善详细设计。 *注 3：“完善”这里是指添加、调整或重构详细设计要素。*
SEC.2.BP6：为架构与详细设计确保一致性和建立双向可追溯性。确保软件架构与软件详细设计之间的一致性并建立双向可追溯性。确保硬件架构组件与硬件详细设计之间的一致性并建立双向可追溯性。
SEC.2.BP7：沟通约定的网络安全实现结果。与所有受影响方沟通约定的网络安全实现结果。 *注 4：沟通的内容可以包括网络安全实现结果和架构中识别的漏洞。*

SEC.2 网络安全实现	成果 1	成果 2	成果 3	成果 4	成果 5	成果 6	成果 7
输出信息项							
04-04 软件架构	X	X					
04-05 软件详细设计		X			X		
04-06 系统架构	X	X					
04-52 硬件架构	X	X					
04-53 硬件详细设计		X			X		
13-51 一致性证据		X				X	

13-52 Communication Evidence							X
15-50 Vulnerability analysis Evidence				X			
17-52 Cybersecurity controls			X				
Base Practices							
BP1: Refine the details of the architecture	X						
BP2: Ensure consistency and establish bidirectional traceability for cybersecurity requirements		X					
BP3: Select cybersecurity controls			X				
BP4: Analyze architecture for weaknesses				X			
BP5: Refine the detailed design					X		
BP6: Ensure consistency and establish bidirectional traceability for architecture and detailed design						X	
BP7: Communicate agreed results of cybersecurity implementation							X

4.3.3. SEC.3 Risk Treatment Verification

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

13-52 沟通证据							X
15-50 漏洞分析证据				X			
17-52 网络安全管控			X				
基本实践							
BP1：完善架构的细节	X						
BP2：为网络安全需求确保一致性和建立双向可追溯性		X					
BP3：选择网络安全管控			X				
BP4：分析架构弱点				X			
BP5：完善详细设计					X		
BP6：为架构与详细设计确保一致性和建立双向可追溯性						X	
BP7：沟通约定的网络安全实现结果							X

4.3.3. SEC.3 风险处理验证

过程 ID
SEC.3
过程名称
风险处理验证
过程目的
其目的是：确认设计的实现和组件的集成符合网络安全需求、已完善的架构设计和详细设计。
过程成果
1) 制订了风险处理验证措施。 2) 根据发布范围选择了验证措施。 3) 验证了设计的实现和组件的集成，记录了验证结果。 4) 建立了风险处理验证措施与网络安全需求之间，以及风险处理验证措施与已完善的架构设计、详细设计和软件单元之间的一致性和双向可追溯性。建立了验证结果与风险处理验证措施之间的双向可追溯性。 5) 总结了风险处理验证结果，并与所有受影响方沟通。

Base practices
SEC.3.BP1: Specify risk treatment verification measures. Specify risk treatment verification measures suitable to provide evidence of compliance of the implementation with the cybersecurity requirements and the refined architectural design and detailed design. *Note 1: The risk treatment verification may provide objective evidence that the outputs of a particular phase of the system, software and hardware development life cycle (e.g., requirements, design, implementation, testing) meet the specified requirements for that phase.* *Note 2: The risk treatment verification measures may further include a check for any unspecified functionality, dynamic verification of control flow and data flow, and static analysis focusing on security coding standards.* *Note 3: The risk treatment verification methods and techniques may include network tests simulating attacks (non-authorized commands, signals with wrong hash key, flooding the connection with messages, etc.), and simulating brute force attacks.* *Note 4: The risk treatment verification methods and techniques may also include audits, review, and other techniques.* *Note 5: Methods of deriving test cases for verification measures may include generation and analysis of equivalence classes, boundary values analysis, and/or error guessing based on knowledge or experience.*
SEC.3.BP2: Select verification measures. Document the selection of verification measures considering selection criteria including criteria for regression verification. The documented selection of verification measures shall have sufficient coverage according to the release scope. *Note 6: Examples for selection criteria can be prioritization of requirements, continuous development, the need for regression verification (due to e.g., changes to the software requirements), or the intended use of the delivered product release (test bench, test track, public road etc.)*
SEC.3.BP3: Perform risk treatment verification activities. Verify the implementation of the design and component integration using the selected risk treatment verification measures. Record the risk treatment verification results including pass/fail status and corresponding verification measure data. *Note 7: See SUP.9 for handling verification results that deviate from expected results.*
SEC.3.BP4: Ensure consistency and establish bidirectional traceability. Ensure consistency and establish bidirectional traceability between the risk treatment verification measures and the cybersecurity requirements. Ensure consistency and establish bidirectional traceability between the risk treatment verification measures and the refined architectural design, detailed design and software units. Establish bidirectional traceability between the verification results and risk treatment verification measures. *Note 8: Bidirectional traceability supports consistency, facilitates impact analysis, and supports demonstration of verification coverage. Traceability alone, e.g., the existence of links, does not necessarily mean that the information is consistent.*
SEC.3.BP5: Summarize and communicate results. Summarize the risk treatment verification results and communicate them to all affected parties. *Note 9: Providing all necessary information from the risk treatment verification execution in a summary enables other parties to judge the consequences.*

基本实践

SEC.3.BP1：定义风险处理验证措施。定义适当的风险处理验证措施，以提供实现符合网络安全需求、已完善的架构设计和详细设计的证据。

注 1：风险处理验证可提供客观证据，即系统、软件和硬件开发生命周期在特定阶段（例如：需求、设计、实现、测试）的输出满足该阶段所定义的需求。

注 2：风险处理验证措施还可包括对任何未定义功能的检查，控制流和数据流的动态验证，以及专用于安全（security）编码标准的静态分析。

注 3：风险处理验证方法和技术可包括网络测试模拟攻击（未授权的指令，携带错误哈希密钥的信号，泛洪攻击等），以及模拟暴力破解攻击。

注 4：风险处理验证方法和技术也可包括审计、评审和其他技术。

注 5：用于验证措施的测试用例的导出方法可包括等价类的生成与分析，边界值分析，和/或基于知识或经验的错误推测。

SEC.3.BP2：选择验证措施。考虑选择准则（包括回归验证准则），记录验证措施选择。所记录的验证措施选择应根据发布范围具备足够的覆盖率。

注 6：选择准则的示例可以是需求优先级，持续开发，回归验证需要（例如由于软件需求变更），或交付产品发布的预期用途（例如，测试台架、测试跑道、公共道路等）。

SEC.3.BP3：执行风险处理验证活动。使用选定的风险处理验证措施，对设计的实现和组件的集成进行验证。记录风险处理验证结果，包括通过/失败状态和相应验证措施数据。

注 7：与预期结果不符的验证结果的处理，参见 SUP.9。

SEC.3.BP4：确保一致性和建立双向可追溯性。确保风险处理验证措施与网络安全需求之间的一致性并建立双向可追溯性。确保风险处理措施与已完善的架构设计、详细设计和软件单元之间的一致性并建立双向可追溯性。建立验证结果与风险处理验证措施之间的双向可追溯性。

注 8：双向可追溯性支持一致性，并有助于影响分析和验证覆盖率的证明。仅有可追溯性本身（如存在两者之间的链接），并不一定意味着两者之间的信息是一致的。

SEC.3.BP5：总结和沟通结果。总结风险处理验证结果，并与所有受影响方沟通。

注 9：在总结中提供来自风险处理验证执行的所有必要信息，以便其他方可以判断结果。

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

4.3.4. SEC.4 Risk Treatment Validation

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

SEC.3 风险处理验证	成果 1	成果 2	成果 3	成果 4	成果 5
输出信息项					
08-60 验证措施	X				
03-50 验证措施数据			X		
08-58 验证措施选择集		X			
15-52 验证结果			X		
13-51 一致性证据				X	
13-52 沟通证据					X
基本实践					
BP1：定义风险处理验证措施	X				
BP2：选择验证措施		X			
BP3：执行风险处理验证活动			X		
BP4：确保一致性和建立双向可追溯性				X	
BP5：总结和沟通结果					X

4.3.4. SEC.4 风险处理确认

过程 ID
SEC.4
过程名称
风险处理确认
过程目的
其目的是：确认集成系统达成相关的网络安全目标。
过程成果
1) 基于网络安全目标定义了风险处理确认措施； 2) 根据定义的准则，包括回归确认准则，选择了确认措施； 3) 使用定义的确认措施对集成系统进行了确认，并记录了确认结果； 4) 建立了确认措施与网络安全目标之间的一致性和双向可追溯；建立了确认结果与确认措施之间的双向可追溯性； 5) 总结了风险处理确认结果，并与所有受影响方沟通。

Base practices
SEC.4.BP1: Specify risk treatment validation measures. Specify the risk treatment validation measures to provide evidence for achievement of the associated cybersecurity goals. *Note 1: Risk treatment validation measures typically use cybersecurity-relevant methods to detect unidentified vulnerabilities (e.g., penetration testing).* *Note 2: Methods of deriving test cases may include generation and analysis of equivalence classes, boundary values analysis, negative tests and/or error guessing based on knowledge or experience.*
SEC.4.BP2: Select validation measures. Document the selection of validation measures according to defined criteria including criteria for regression validation. The documented selection of validation measures shall have sufficient coverage of the cybersecurity goals.
SEC.4.BP3: Perform risk treatment validation activities. Validate the integrated system using the selected risk treatment validation measures. Record the validation results and corresponding validation measure data. *Note 3: See SUP.9 for handling validation results that deviate from expected results.*
SEC.4.BP4: Ensure consistency and establish bidirectional traceability. Ensure consistency and establish bidirectional traceability between risk treatment validation measures and cybersecurity goals. Establish bidirectional traceability between validation results and validation measures. *Note 4: Bidirectional traceability supports consistency, facilitates impact analysis, and supports demonstration of validation coverage. Traceability alone, e.g., the existence of links, does not necessarily mean that the information is consistent.*
SEC.4.BP5 Summarize and communicate results. Summarize the risk treatment validation results and communicate them to all affected parties. *Note 5: This may include information from the risk treatment validation activities and important findings concerning additional vulnerabilities to enable other parties to judge the consequences.*

基本实践
SEC.4.BP1：定义风险处理确认措施。定义风险处理确认措施以提供达成相关的网络安全目标的证据。 *注 1：风险处理确认措施通常使用与网络安全相关的方法来探测未识别的漏洞（例如，渗透测试）。* *注 2：测试用例导出方法可包括等价类的生成与分析，边界值分析，负面测试，和/或基于知识或经验的错误推测。*
SEC.4.BP2：选择确认措施。根据定义的准则（包括回归确认准则），记录确认措施的选择。所记录的确认措施选择应针对网络安全目标具备足够的覆盖率。
SEC.4.BP3：执行风险处理确认活动。使用选定的风险处理确认措施对集成的系统进行确认。记录确认结果以及相应确认措施数据。 *注 3：与预期结果不符的确认结果的处理，参见 SUP.9。*
SEC.4.BP4：确保一致性和建立双向可追溯性。确保风险处理确认措施与网络安全目标之间的一致性并建立双向可追溯性。建立确认结果与确认措施之间的双向可追溯性。 *注 4：双向可追溯性支持一致性，并有助于影响分析和确认覆盖率的证明。仅有可追溯性本身（如存在两者之间的链接），并不一定意味着两者之间的信息是一致的。*
SEC.4.BP5：总结和沟通结果。总结风险处理确认结果，并与所有受影响方沟通。 *注 5：该实践可包括来自风险处理确认活动的信息以及关于额外漏洞的重要发现，以便其他方可以判断结果。*

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

SEC.4 风险处理确认	成果 1	成果 2	成果 3	成果 4	成果 5
输出信息项					
08-59 确认措施	X				
03-55 确认措施数据			X		
08-57 确认措施选择集		X			
13-24 确认结果			X		
13-51 一致性证据				X	
13-52 沟通证据					X
基本实践					
BP1：定义风险处理确认措施	X				
BP2：选择确认措施		X			
BP3：执行风险处理确认活动			X		
BP4：确保一致性和建立双向可追溯性				X	
BP5：总结和沟通结果					X

Annex A – Process Assessment and Reference Model Conformity

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

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

Annex B – Information Item Characteristics

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

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

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

Table B.2 — Information Item Characteristics

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

ID	Name	Characteristics
02-01	Commitment/ agreement	• Signed off by all parties involved in the commitment/agreement • Establishes what the commitment is for • Establishes the resources required to fulfill the commitment, such as: - time - people - budget - equipment - facilities
02-50	Interface agreement	• Interface agreement should include definitions regarding - customer and supplier stakeholders and contacts - tailoring agreements - customer/supplier responsibilities (e.g., roles, RASIC chart) for distributed activities, including required actions in development and post-development - share of information/work products in case of issues (e.g., vulnerabilities, findings, risks) - agreed customer/supplier milestones - duration of supplier's support and maintenance

附录 A – 过程评估和参考模型的符合性

给定的过程评估和参考模型与 Automotive SPICE® 4.0 核心模型中的声明和定义保持一致。因此，适用 Automotive SPICE®过程参考和评估模型（4.0 版）附录 A 中给出的符合性声明。[Automotive Spice® 4.0]

附录 B – 信息项特性

信息项特性使用表 B.1 模式进行了定义。详见 Automotive SPICE® 4.0 第 3.3.2 章节中关于如何诠释信息项，及其特性的定义和解释。

表 B.1 — 信息项特性(IIC)的结构

信息项 ID	用于引用信息项的标识编号。
信息项名称	提供与信息项特性相关联的典型名称的示例。此名称是由实践或过程可产出的信息项的类型的标识。组织可使用其他名称来命名这些信息项。在组织中信息项的名称并不重要。同样，组织可有多个等效的信息项而包含一个信息项类型中所定义的特性。信息项的格式可多种多样。由评估师和组织单位协调员，将其组织所产出的实际信息项映射到这里给出的示例。
信息项特性	提供与信息项类型相关联的潜在特性的示例。评估师可在评估组织单位所提供的样例的过程中使用这些特性。其意图并不是将所罗列的特性作为检查单进行使用。在被评估的组织中，可能发现某些特性被包含在其他工作产品中是恰当的。

表 B.2 — 信息项特性

本表格仅包含 Automotive SPICE®网络安全相关的信息项特性。

ID	名称	特性
02-01	承诺/协议	• 由承诺/协议的所有参与方签署 • 建立对什么的承诺 • 建立为满足承诺所需的资源，例如： - 时间 - 人 - 预算 - 设备 - 设施
02-50	接口协议	• 接口协议应包括以下定义 - 客户与供应商利益相关方及联系人 - 裁剪协议 - 客户/供应商针对所分配的活动（包括开发和开发后所需的行动）的职责（例如，角色，RASIC 图表） - 在出现问题时（例如，漏洞，发现，风险）信息/工作产品的共享 - 约定的客户/供应商里程碑 - 供应商支持和维护的期限

03-50	Verification measure data	• Verification measure data are data recorded during the execution of a verification measure, e.g.: - for test cases: raw data, logs, traces, tool generated outputs - measurements: values - calculations: values - simulations: protocol - reviews such as optical inspections and findings record - analyses: values
03-55	Validation measure data	• Validation measure data are data recorded during the execution of a validation measure, e.g.: Logs, traces, raw data, crash dumps, review protocols.
04-04	Software architecture	• A justifying rationale for the chosen architecture. • Individual functional and non-functional behavior of the software components • Settings for application parameters (being a technical implementation solution for configurability-oriented requirements) • Technical characteristics of interfaces for relationships between software components such as: - Synchronization of Processes and tasks - Programming language call - APIs - Specifications of SW libraries - Method definitions in an object- oriented class definitions or UML/SysML interface classes - Callback functions, “hooks” • Dynamics of software components and software states such as: - Logical software operating modes (e.g., start-up, shutdown, normal mode, calibration, diagnosis, etc.) - intercommunication (processes, tasks, threads) and priority - time slices and cycle time - interrupts with their priorities - interactions between software components • Explanatory annotations, e.g., with natural language, for single elements or entire diagrams/models.
04-05	Software detailed design	• Elements of a software detailed design: - Control flow definition - Format of input/output data - Algorithms - Defined data structures - Justified global variables - Explanatory annotations, e.g., with natural language, for single elements or entire diagrams/models • Examples for expression languages, depending on the complexity or criticality of a software unit: - natural language or informal languages - semi-formal languages (e.g., UML, SysML) - formal languages (e.g., model-based approach)

03-50	验证措施数据	• 验证措施数据是在执行验证措施中记录的数据，例如: - 关于测试用例：原始数据、日志、记录、工具生成的输出 - 测量：值 - 计算: 值 - 仿真: 协议 - 评审例如光学检测，发现记录 - 分析: 值
03-55	确认措施数据	• 确认措施数据是在执行确认措施中记录的数据，例如，日志、记录、原始数据、崩溃转储、评审记录。
04-04	软件架构	• 所选架构的合理依据 • 软件组件的单独功能性和非功能性行为 • 应用参数的设置（作为面向配置需求的技术实现方案） • 软件组件间关联接口的技术特性，例如： - 进程和任务的同步 - 编程语言调用 - API 函数 - 软件库的规范 - 面向对象类定义中的方法定义或者 UML/SysML 接口类 - 回调函数，“钩子函数（Hooks）” • 软件组件以及软件状态的动态，例如： - 逻辑软件运行模式（例如:启动、关机、正常模式、标定和诊断等） - 内部通信（进程，任务，线程）以及优先级 - 时间片和周期时间 - 中断及其优先级 - 软件组件间交互 • 解释性注释，例如，使用自然语言，用于单个要素或整个图表/模型。
04-05	软件详细设计	• 软件详细设计的要素： - 控制流定义 - 输入/输出数据格式 - 算法 - 定义的数据结构 - 合理的全局变量 - 解释性注释，例如，使用自然语言，用于单个要素或整个图表/模型。 • 表达式语言的示例，取决于软件单元的复杂性或关键性： - 自然语言或非正式语言 - 半形式语言（例如，UML、SysML） - 形式语言（例如，基于模型的方法）

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

04-06	系统架构	• 所选架构的合理依据 • 系统要素的单独行为 • 系统要素间的关联关系 - 系统参数的设置（例如应用参数） - 手动/人工控制操作，例如：按照 STPA • 接口定义 - 两个系统要素间关联接口的技术特性 • 系统要素间接口，例如： - 总线接口 (CAN, MOST, LIN, Flexray 等) - 热影响 - 软硬件接口(HSI), 见下文 - 电磁接口 - 光接口 - 硬件-机械接口（例如：同时满足机械和电气需求的线束, PCB 的外壳接口） - 硬件-机械互连技术，如接插件，无焊压接 - 爬电距离和电气间隙 • 固定装置，如粘接接头、螺钉螺栓/配件、铆接螺栓、焊接 • 电子电气硬件相关系统接口，例如： - 模拟或数字接口（PWM, I/O）及其引脚配置 - SPI 总线, I2C 总线, 电气互连 - 放置，例如：硬件要素间的热接口（散热） - 软焊 - 爬电距离和电气间隙 • 机械工程的接口，例如： - 摩擦 - 热影响 - 公差 - 离合器 - 固定装置，如粘接接头、螺钉螺栓/配件、铆接螺栓、焊接 - 力（例如振动或摩擦造成的力） - 放置 - 形状 • 软硬件接口，例如： - 用于µCs/MOSFET 的连接器的引脚配置和浮接输入输出 - 由应用软件所反映的信号缩放和分辨率 • 机械-硬件接口，例如 - 如机械尺寸 - 接插件位置 - 位置，例如: 霍尔传感器相对于母线的定位 - 公差 • 系统要素以及系统状态的动态： - 描述系统状态和运行模式（启动、关机、休眠模式、诊断/标定模式、生产模式、降级、紧急如“跛行”等） - 描述关于运行模式的系统组件间依赖关系 - 系统要素间的交互，例如由 ECU 所反映的机械组件的惯性、信号传播以及通过硬件和软件（例如总线系统）的处理时间 • 解释性注释，例如，使用自然语言，用于单个要素或整个图表/模型。

04-52	Hardware architecture	• Describes the initial floor plan and the overall hardware structure • Identifies the required hardware components • Includes the rationale for chosen options of hardware architecture • Identifies own developed and supplied hardware components • Identifies the required internal and external hardware component interfaces • Specifies the interfaces of the hardware components • Specifies dynamic behavior • Identifies the relationship and dependency between hardware components • Describes all hardware variants to be developed • Describes power supply, thermal and grounding concepts
04-53	Hardware detailed design	• Describes the interconnections between the hardware parts • Specifies the interfaces of the hardware parts • Specifies the dynamic behavior (examples are: transitions between electrical states of hardware parts, power-up and power-down sequences, frequencies, modulations, signal delays, debounce times, filters, short circuit behavior, self-protection) • Describes the conclusions and decisions based on e.g., analysis reports, datasheets, application notes • Describes the constraints for layout
08-55	Risk treatment	• Identifies - the risk to be mitigated, avoided, retained or transferred (shared) - the activities to mitigate, avoid, retain or transfer (share) the risk - the originator of the measure - criteria for successful implementation - criteria for cancellation of activities - frequency of monitoring • Risk treatment alternatives: - treatment option selected- avoid/reduce/retain/ transfer (share) - alternative descriptions - recommended alternative(s) • justifications
08-57	Validation measure selection set	• Include criteria for re-validation in the case of changes (regression). • Identification of validation measures, also for regression
08-58	Verification measure selection set	• Include criteria for re-verification in the case of changes (regression). • Identification of verification measures, also for regression testing

04-52	硬件架构	• 描述初始平面图和整体硬件结构 • 识别所需的硬件组件 • 包含所选硬件架构选项的依据 • 识别自主开发和被提供的硬件组件 • 识别所需的内部和外部硬件组件的接口 • 定义硬件组件的接口 • 定义动态行为 • 识别硬件组件间的关系和依赖关系 • 描述需要开发的所有硬件的变体 • 描述电源，热和接地概念设计
04-53	硬件详细设计	• 描述硬件元器件间的关连 • 定义硬件元器件的接口 • 定义动态行为（例如：硬件元器件电气状态之间的迁移、上电和下电时序、频率、调制、信号延迟、去抖动时间、滤波器、短路行为、自我保护） • 描述基于例如分析报告、数据表、应用说明等的结论和决策 • 描述布局的约束
08-55	风险措施	• 识别 - 需要缓解、避免、保留或转移（分担）的风险 - 缓解、避免、保留或转移（分担）风险的活动 - 措施的发起人 - 成功实施的准则 - 取消活动的准则 - 监测频率 • 风险处理备选方案: - 选择处理方案 - 避免/降低/保留/转移(分担) - 备选方案描述 - 推荐的备选方案 - 理由
08-57	确认措施选择集	• 包括在发生变更（回归）情况下的重新确认的准则。 • 识别确认措施，也适用回归
08-58	验证措施选择集	• 包括在发生变更（回归）情况下的重新验证的准则。 • 识别验证措施，也适用回归测试

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 • Cybersecurity responsibilities of the supplier • The scope of work regarding cybersecurity, including the cybersecurity goals or the set of relevant cybersecurity requirements and their attributes • Action plan for identified deviations and risks • Identifies desired characteristics, such as: - system architecture, configuration requirements or the requirements for service (consultants, maintenance, etc.) - quality criteria or requirements - project schedule requirements - expected delivery/service dates - cost/price expectations - regulatory standards/requirements • Identifies submission constraints: - date for resubmission of the response • requirements with regard to the format of response
13-24	Validation results	• Validation data, logs, feedback, or documentation • Validation measure passed • Validation measure not passed • Validation measure not executed, and a rationale • Information about the validation execution (date, participants etc.) • Abstraction or summary of validation results

08-59	确认措施	• 确认措施可以为测试用例、测量、仿真、模拟或最终用户调查 • 确认措施的规范包含 - 确认措施的通过/失败准则(完成和结束准则) - 确认措施的准入和准出准则，以及中止和重启的准则的定义 • 技术 • 必要的确认环境和基础设施 • 必要的顺序或排序
08-60	验证措施	• 验证措施可以为测试用例、测量、计算、仿真、评审、光学检测或分析 • 验证措施的规范包含 - 验证措施的通过/失败准则(完成和结束准则) - 验证措施的准入和准出准则，以及中止和重启的准则的定义 • 技术（例如黑盒 和/或 白盒测试、等价类和边界值、功能安全的故障注入，网络安全的渗透测试、基于模型开发的背靠背测试、ICT） • 必要的验证环境和基础设施 • 必要的顺序或排序
12-01	报价请求	• 引用需求规范 • 供应商的网络安全职责 • 网络安全的工作范围，包括网络安全目标或相关网络安全需求及其属性 • 针对已识别偏差和风险的行动计划 • 识别希望的特性，如： - 系统架构、配置需求或服务需求（咨询、维护等） - 质量准则或需求 - 项目进度需求 - 期望的交付/服务日期 - 成本/价格期望 - 法规标准/需求 • 识别提交约束： - 重新提交响应的日期 • 关于响应格式的需求
13-24	确认结果	• 确认数据、日志、反馈或文档 • 通过的确认措施 • 未通过的确认措施 • 未执行的确认措施和依据 • 关于确认的执行信息（日期，参与者等） • 确认结果的摘要或总结

13-51	Consistency evidence	• Demonstrates bidirectional traceability between artifacts or information in artifacts, throughout all phases of the life cycle, by e.g., - tool links - hyperlinks - editorial references - naming conventions • Evidence that the content of the referenced or mapped information coheres semantically along the traceability chain, e.g., by - performing pair working or group work - reviewing by peers, e.g., spot checks - maintaining revision history in documents - providing change commenting (via e.g., meta-information) of database or repository entries • *Note: This evidence can be accompanied by e.g., Definition of Done (DoD) approaches.*
13-52	Communication evidence	• All forms of interpersonal communication such as - e-mails, also automatically generated ones - tool-supported workflows - meeting, verbally or via meeting minutes (e.g., daily standups) - podcast - blog - videos - forum - live chat - wikis - photo protocol
14-02	Corrective action	• Identifies the initial problem • Identifies the ownership for completion of defined action • Defines a solution (series of actions to fix problem) • Identifies the open date and target closure date • Contains a status indicator • Indicates follow up audit actions
15-09	Risk status	• Identifies the status, or the change, of an identified risk: - risk statement - risk source - risk impact and risk likelihood - categories and risk thresholds, e.g., for prioritization or setting a status - risk treatment activities in progress
15-21	Supplier evaluation	• States the purpose of evaluation • Identifies supplier selection criteria • Method and instrument (checklist, tool) used for evaluation • Requirements used for the evaluation • Assumptions and limitations • Identifies the context and scope information required (e.g., date of evaluation, parties involved) • Fulfillment of evaluation requirements
15-50	Vulnerability analysis evidence	• Identifies - ID - description - attack path concerned • attack feasibility (e.g., CVSS (Common Vulnerability Scoring System) rating)

13-51	一致性证据	• 在生命周期的所有阶段，通过以下方式展示制品或制品中信息之间的双向可追溯性 - 工具链接 - 超链接 - 编辑参考文献 - 命名规则 • 所引用或映射的信息内容在语义上与追溯链上的信息一致的证据，例如 - 执行结对或分组工作 - 由同行执行，例如抽查 - 维护文档中的修订历史 - 提供数据库或存储库条目的更改注释（例如，通过元信息） *注意：此证据可以结合例如完成定义（DoD）方法。*
13-52	沟通证据	• 所有形式的人际沟通，如： - 电子邮件，同样适用自动生成的 - 工具支持的工作流 - 会议，口头或会议记录(例如：每日站会) - 播客 - 博客 - 视频 - 论坛 - 即时聊天 - 维基 - 照片协议
14-02	纠正行动	• 识别初始问题 • 识别已定义行动完成的所有权 • 定义解决方案（解决问题的一系列行动） • 识别提出日期和目标关闭日期 • 包含状态指示器 • 指示后续审核行动
15-09	风险状态	• 识别已识别风险的状态，或者变化: - 风险陈述 - 风险源 - 风险影响和风险概率 - 归类和风险阈值，例如：优先级排序或状态设定 - 正在进行的风险处理活动
15-21	供应商评估	• 陈述评估的目的 • 确认供应商选择准则 • 评估使用的方法和工具（检查表，工具） • 评估所使用的需求 • 假设和限制 • 识别所需的背景和范围信息（例如，评估的时间，涉及的相关方） • 评估需求的满足
15-50	漏洞分析证据	• 识别 - ID - 描述 - 有关攻击路径 • 攻击可行性（例如，CVSS 评级（通用漏洞评分系统））

15-51	Analysis results	• Identification of the object under analysis. • The analysis criteria used, e.g.: - selection criteria or prioritization scheme used - decision criteria - quality criteria • The analysis results, e.g.: - what was decided/selected - reason for the selection - assumptions made - potential negative impact • Aspects of the analysis may include - correctness - understandability - verifiability - feasibility - validity
15-52	Verification Results	• Verification data and logs • Verification measure passed • Verification measure not passed • Verification measure not executed • information about the test execution (date, tester name etc.) • Abstraction or summary of verification results

15-51	分析结果	• 识别分析对象。 • 使用的分析准则，例如： - 使用的选择准则或优先级排序方式 - 决策准则 - 质量准则 • 分析结果，例如： - 决定/选择的是什么 - 选择理由 - 所作的假设 - 潜在负面影响 • 分析方面可能包括 - 正确性 - 可理解性 - 可验证性 - 可行性 - 有效性
15-52	验证结果	• 验证数据和日志 • 通过的验证措施 • 未通过的验证措施 • 未执行的验证措施和理由 • 关于验证的执行信息（日期，测试人员姓名等） • 验证结果的概述或总结

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 of requirements aspects at the system level are thermal characteristics such as - heat dissipation - dimensions - weight - materials • Examples of aspects related to requirements about system interfaces are - connectors - cables - housing • Examples of requirements at the hardware level are - lifetime and mission profile, lifetime robustness - maximum price - storage and transportation requirements - functional behavior of analog or digital circuits and logic - quiescent current, voltage impulse responsiveness to crank, start-stop, drop-out, load dump - temperature, maximum hardware heat dissipation - power consumption depending on the operating state such as sleep-mode, start-up, reset conditions - frequencies, modulation, signal delays, filters, control loops - power-up and power-down sequences, accuracy and precision of signal acquisition or signal processing time - computing resources such as memory space and CPU clock tolerances - maximum abrasive wear and shearing forces for e.g., pins or soldering joints - requirements resulting from lessons learned - safety related requirements derived from the technical safety concept

17-00	需求	• 对功能以及能力（例如：非功能性需求），或其接口之一的期待 - 从黑盒的视角 - 可被验证的，不暗示设计或实现决策的，无歧义的，并和其他需求无矛盾。 • 暗示或表示设计或实现决策的需求陈述称为“设计约束”。 • 系统层级需求方面的示例如热特性，如 - 散热 - 尺寸 - 重量 - 材料 • 关于系统接口方面的需求示例如 - 接插件 - 线束 - 外壳 • 硬件层级需求的示例 - 寿命和任务剖面，寿命可靠性 - 最高价格 - 存储和运输需求 - 模拟或数字电路和逻辑的功能行为 - 静态电流，电压脉冲对点火、启停、压差，负荷突降的响应 - 温度，最大硬件散热 - 依赖于工作状态的功耗，如睡眠模式、启动、复位条件 - 频率、调制、信号延迟、滤波器、控制环路 - 上电和断电时序、信号采集或信号处理时间的准确度和精度 - 计算资源，如内存空间和 CPU 时钟容差 - 最大磨料磨损和剪切力，例如引脚或焊点 - 从经验教训中得出的需求 - 从技术安全概念推导出的安全相关需求

17-51	Cybersecurity goals	• Describe a property of an asset that it is necessary to protect by means of cybersecurity • This may include - Confidentiality needs - Authorization needs - Integrity needs - Availability needs - etc. • Information that can be included in the goals: - Goal Title - Objective - Scope - Key Metrics and success criteria - Milestones (if Applicable) - Action plan (if applicable) - stakeholders involved - link to potential risks - budget and resources - Timeline - Compliance and standards - Sign-off and approval
17-52	Cybersecurity controls	• Technical solutions to prevent, detect, or mitigate cybersecurity risks • Associated to one or more cybersecurity requirements
17-53	Cybersecurity threat scenario	• Description of how threats exploit a weakness/vulnerability or multiple weaknesses/vulnerabilities exposing assets to harm, to enable the corresponding risk analysis • Detailed chronological and functional description of an actual or hypothetical threat or group of threats • Sequence of actions that involve interaction with system resulting in a threat scenario • A threat scenario shall include, e.g. - asset targeted by the threat - cybersecurity property which is compromised - compromise cause of the cybersecurity property • Threat scenarios give a detailed and concrete description of applicable threats, like: - ransomware - phishing - spoofing - denial of service
17-54	Requirement attribute	• Meta-attributes that support structuring and definition of release scopes of requirements. • Can be realized by means of tools. • *Note*: *usage of requirements attributes may further support analysis of requirements.*
18-50	Supplier evaluation criteria	• Expectations for conformity, to be fulfilled by suppliers • Links from the expectations to national/international/domain-specific standards/laws/regulations • Requirements' conformity evidence to be provided by the potential suppliers or assessed by the acquiring organization • agreed exceptions to the requirements

17-51	网络安全目标	• 描述需要通过网络安全措施保护的资产的属性 • 其可能包括 - 保密需求 - 授权需求 - 完整性需求 - 可用性需求 - 等。 • 目标中可包括的信息 - 目标标题 - 目的 - 范围 - 关键指标和成功准则 - 里程碑（如适用） - 行动计划（如适用） - 所设计的利益相关方 - 潜在的风险链接 - 预算和资源 - 时间计划 - 合规性和标准 - 签署和审批
17-52	网络安全管控	• 预防，探测或缓解网络安全风险的技术方案 • 与一个或多个网络安全需求相关联
17-53	网络安全威胁场景	• 对威胁如何利用一个或多个弱点/漏洞使资产收到损害，以进行相应的风险分析的说明 • 对实际或假设的（一组）威胁的详细时间和功能的说明 • 涉及与系统交互导致威胁场景的行动序列 • 威胁场景应包括，例如： - 威胁所针对的资产 - 收到损害的网络安全属性 - 网络安全属性的损害原因 • 威胁场景对适用的威胁给出详细而具体的描述，例如： - 勒索软件 - 网络钓鱼 - 欺骗 - 拒绝服务
17-54	需求属性	• 支持需求发布范围的结构化和定义的元属性（Meta-attributes）。 • 可以通过工具实现。 • *注意：使用需求属性可以进一步支持需求分析。*
18-50	供应商评估准则	• 由供应商履行的对符合性的期望 • 从期望到国家/国际/特定领域的标准/法律/法规的关联 • 由潜在供应商或者采购组织通过评估提供的需求符合性的证据 • 针对需求的裁剪或例外的规定

Annex C – Terminology

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

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

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

Table C.1 — Terminology

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

附录 C – 术语

Automotive SPICE® 遵循以下术语使用的优先顺序：

a) ISO/IEC 33001 评估相关的术语
b) ISO/IEC/IEEE 24765 和 ISO/IEC/IEEE 29119 的术语（见附录 C）
c) Automotive SPICE®引入的术语（见附录 C）
d) ISO/SAE 21434 网络安全相关的术语

附录 C 列出了从 ISO/IEC/IEEE 24765 和 ISO/IEC/IEEE 29119 引用的适用术语。它还提供了在 Automotive SPICE 中专门定义的术语。其中有些定义是基于 ISO/IEC/IEEE 24765。

表 C.1 — 术语

术语	来源	描述
验收测试	ISO/IEC/IEEE 24765	能够让用户、客户或授权方确定是否接受系统或组件而执行的正式测试。
应用参数	Automotive SPICE® 4.0	应用参数是软件变量，其中包含可以在系统或软件层级进行更改的数据；它们影响系统或软件的行为和属性。应用参数的概念有两种表达方式： • 规范（分别包括名变量名、域值范围、技术数据类型、默认值、物理单位（如适用）、对应的内存映射）。 • 通过数据应用接收的实际定量数据值。 • 应用参数并非需求本身，而是一种针对可配置性导向需求的技术实现方案。
架构要素	Automotive SPICE® 4.0	在系统和软件层级架构分解的结果： • 将系统分解为适当的各层级上的系统架构要素。 • 将软件分解为适当的各层级上的软件架构要素至软件组件（软件架构的最低层级的要素）。
资产	ISO/SAE 21434	有价值或对价值有贡献的对象
攻击路径	ISO/SAE 21434	为实现威胁场景的一系列刻意为之的行动
攻击可行性	ISO/SAE 21434	攻击路径的属性，用来描述成功实施一系列相应行动的容易性
黑盒测试	Automotive SPICE® 4.0	需求测试方法，该测试开发无需了解被测试项的内部结构和机制。
代码评审	Automotive SPICE® 4.0	由一位或多位有资质人员检查代码，以确定是否适合预期用途并识别与规范和标准的不符合项。
编码	ISO/IEC/IEEE 24765	将设计规范（设计描述）中的逻辑和数据转换成编程语言。

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

一致性	Automotive SPICE® 4.0	一致性涉及内容和语义，确保工作产品之间没有互相矛盾。一致性由双向可追溯性支持。
网络安全事件	ISO/SAE 21434	与某个相关项或组件相关的网络安全信息。
网络安全目标	ISO/SAE 21434	与一个或多个威胁场景相关的概念层级的网络安全需求。
网络安全信息	ISO/SAE 21434	尚未确定的网络安全相关信息。
网络安全属性	ISO/SAE 21434	值得保护的属性。
损害场景	Automotive SPICE® 4.0	涉及车辆和车辆功能并影响道路使用者的不良后果。
要素	Automotive SPICE® 4.0	要素是在"V"模型左边的架构和设计层级上的所有结构化对象。这样的要素可以被进一步分解为在架构或设计各适当层级上更细的子要素。
错误	ISO/IEC/IEEE 24765	计算值、观测值、测量值或条件与真实值、指定值、逻辑上的正确值或条件之间的差值。
故障	ISO/IEC/IEEE 24765	软件中错误的表现。
功能性需求	ISO/IEC/IEEE 24765	识别产品或过程对于产生所需的行为和/或结果所必须完成的内容的陈述。
硬件	ISO/IEC/IEEE 24765	用来处理、存储或转换计算机程序或数据的物理设备。
集成	Automotive SPICE® 4.0	将项组合成为更大的项直至成为整个系统的过程。
相关项	ISO 21434	在整车层级实现一个功能的一个组件或一组组件。
质量保证	ISO/IEC/IEEE 24765	对所有必要行动采取计划的和系统化的模式，以提供充分的信心说明某个项或产品符合已建立的技术需求。
回归测试	Automotive SPICE® 4.0	对系统或项进行选择性的再测试，以验证修改没有造成意外的影响，并且系统或项还是符合所定义的需求。
需求	Automotive SPICE® 4.0	为满足合同、标准、规范或其他正式的文档要求，系统、系统项、产品或服务必须达到或具有的属性或能力。
需求规范	Automotive SPICE® 4.0	为系统或项定义需求的文件。通常包括功能性需求、性能需求、接口需求，设计需求和开发标准。
软件	ISO/IEC/IEEE 24765	计算机程序、规程和可能相关的操作计算机系统的文档和数据。

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

软件组件	Automotive SPICE® 4.0	面向设计和实施过程的软件组件： 软件架构将软件分解为跨适当层级的软件组件，直至概念模型中的最低层级的软件组件。 面向验证过程的软件组件： 在验证中的软件组件的实现表示为，例如，源代码、目标文件、库文件、可执行文件或可执行模型。
软件要素	Automotive SPICE® 4.0	参见软件组件或软件单元。
软件单元	Automotive SPICE® 4.0	面向设计和实施过程的软件单元： 作为软件组件分解的结果，软件被分解为软件单元，其是软件要素的表示并决定不再细分，并且是概念模型中最低级别的软件组件的一部分。 面向验证过程的软件单元： 在验证中的软件单元表示为例如，源代码、目标文件、库文件、可执行文件或可执行模型。
静态分析	Automotive SPICE® 4.0	基于形式、结构、内容或文档评价项的过程。
系统	Automotive SPICE® 4.0	将一组交互项组织在一起，为完成在特定的环境下的某一特定的功能或一组功能。
测试	Automotive SPICE® 4.0	在特定条件下对于项（系统、硬件或软件）所执行的活动，并记录、总结和沟通结果。
威胁场景	ISO/SAE 21434	可能导致一个或多个资产的网络安全属性受损、并由此触发损害场景的潜在原因。
追溯性	ISO/IEC/IEEE 24765	在两个或多个开发过程产品之间建立关联性的程度，尤其是互相之间有前-后或主-从关系的产品。
单元	Automotive SPICE® 4.0	不能被进一步分解的软件组件。 → [软件组件]
单元测试	Automotive SPICE® 4.0	对单个软件单元或一组组合的软件单元的测试。
确认	ISO/IEC/IEEE 29119	确认证明了工作项可以被用户用于他们特有的任务。
验证	ISO/IEC/IEEE 29119	验证是通过提供客观的证据来确认定义的需求被指定的工作项所满足。
漏洞	ISO/SAE 21434	可以作为攻击路径一部分而被利用的弱点。
弱点	ISO/SAE 21434	可能导致不良行为的缺陷或特征。
白盒测试	Automotive SPICE® 4.0	基于对测试项的内部结构和机制的了解，开发测试的测试方法。

Table C.2— Abbreviations / 表 C.2 — 缩写

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

Annex D – Traceability and Consistency

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

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

Furthermore, bidirectional traceability has been explicitly defined between

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

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

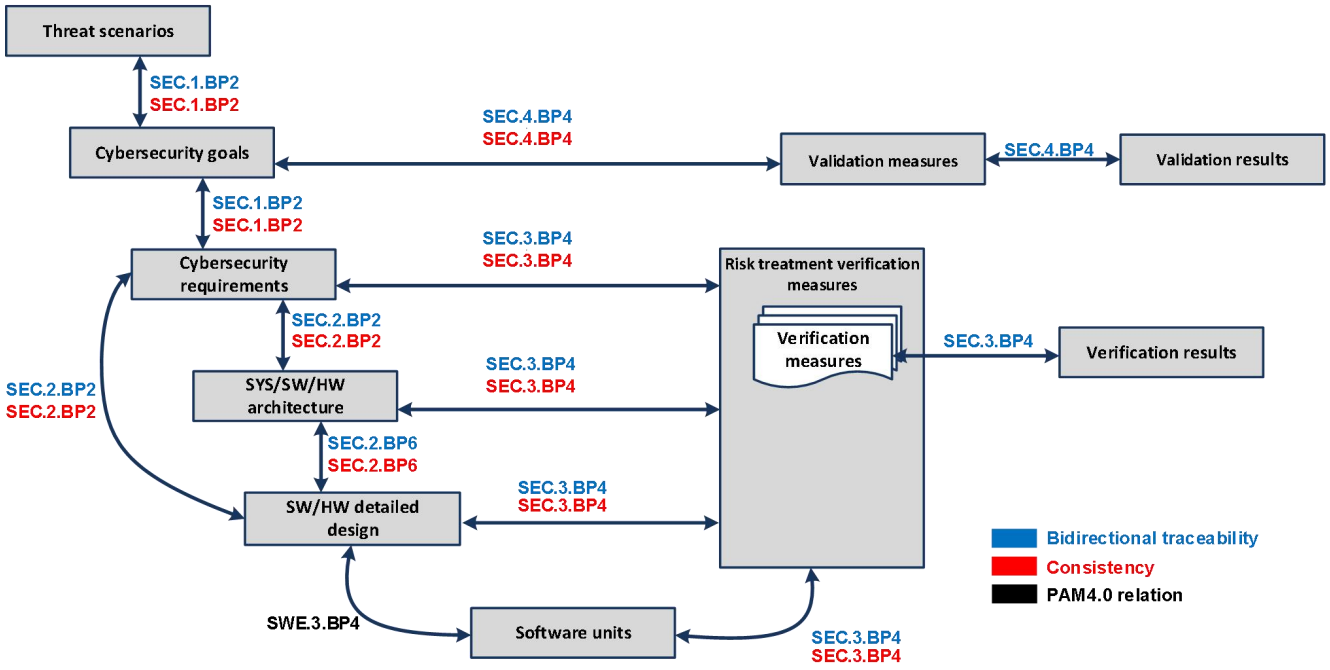

Figure 5 — Bidirectional Traceability and Consistency

附录 D – 可追溯性和一致性

在 Automotive SPICE® 网络安全 和 Automotive SPICE® 4.0 中，可追溯性和一致性均通过一个单独的基本实践来阐述。

可追溯性是指在工作产品之间存在引用或关联，从而进一步支持覆盖性、影响分析、需求实现状态跟踪等方面。相对而言，一致性所关注的是内容和语义。

此外，以下各项之间的双向可追溯性得到明确定义：

- 威胁场景和网络安全目标
- 网络安全目标和确认规范
- 网络安全需求/架构/软件详细设计/硬件详细设计和风险处理验证规范
- 确认规范和确认结果，以及
- 验证措施和验证结果。

下图展示了双向可追溯性和一致性的概览。

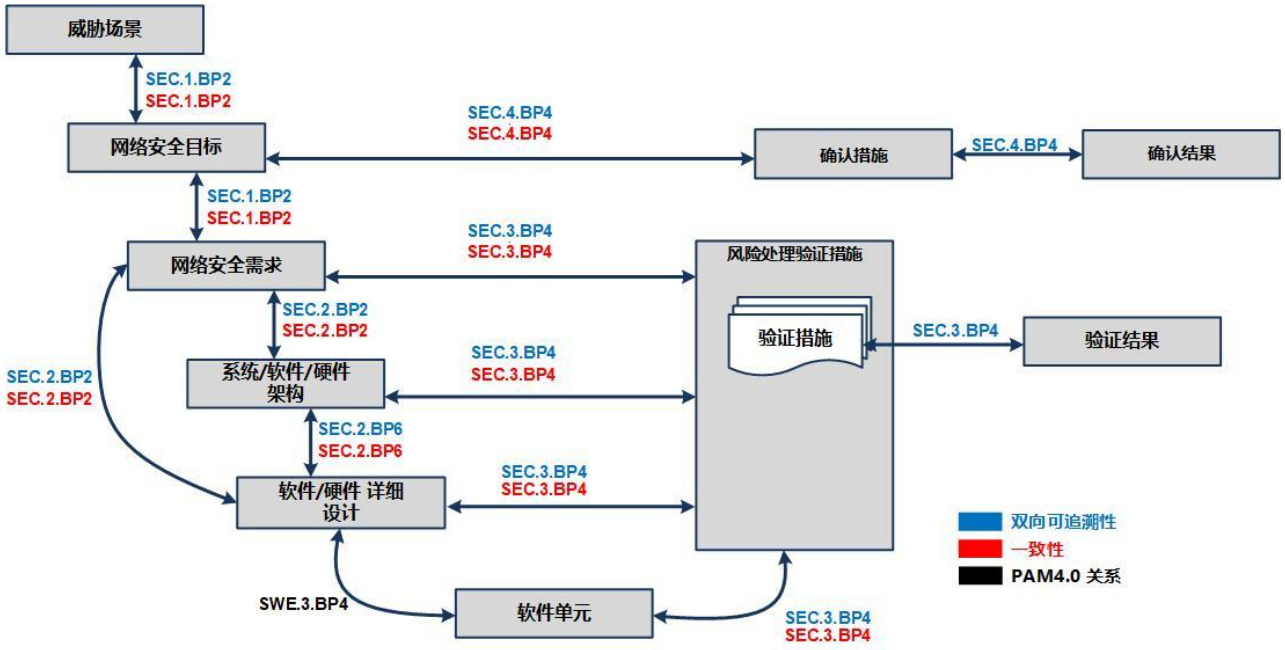

图 5 — 双向可追溯性和一致性

Annex E– General Concept of Automotive SPICE® for Cybersecurity

In this Annex the relationship between Automotive SPICE® for Cybersecurity and ISO/SAE 21434 is described. 图 14 shows the base practices of Automotive SPICE® for Cybersecurity with the respective IIC or work products and the respective requirement [RQ] in the ISO/SAE 21434.

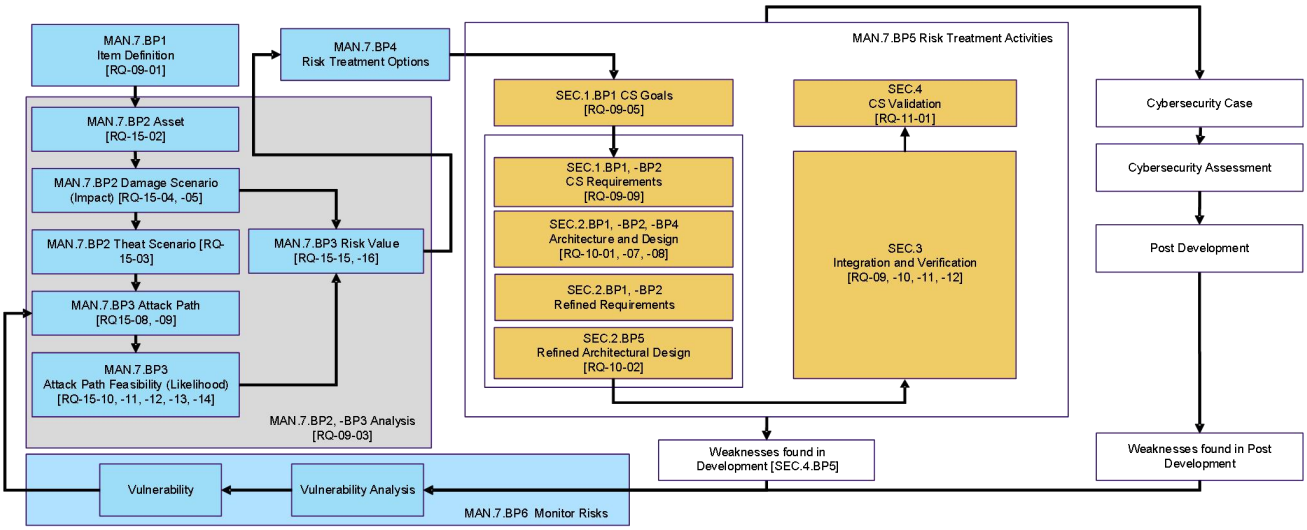

Figure 6 — Automotive SPICE® for Cybersecurity general concept

附录 E – Automotive SPICE® 网络安全通用概念

本附件介绍了 Automotive SPICE®网络安全和 ISO/SAE 21434 之间的关系。图 7 展示了 Automotive SPICE®网络安全的基本实践及其相应 IIC 或工作产品，和 ISO/SAE 21434 的相应要求 [RQ]。

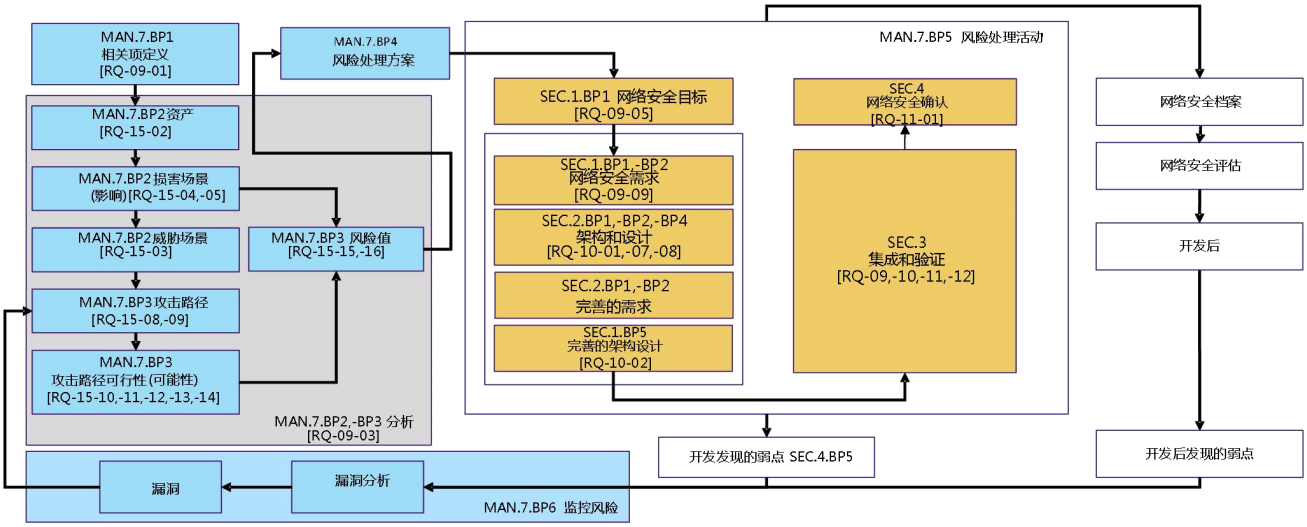

图 6 — Automotive SPICE® 网络安全通用概念