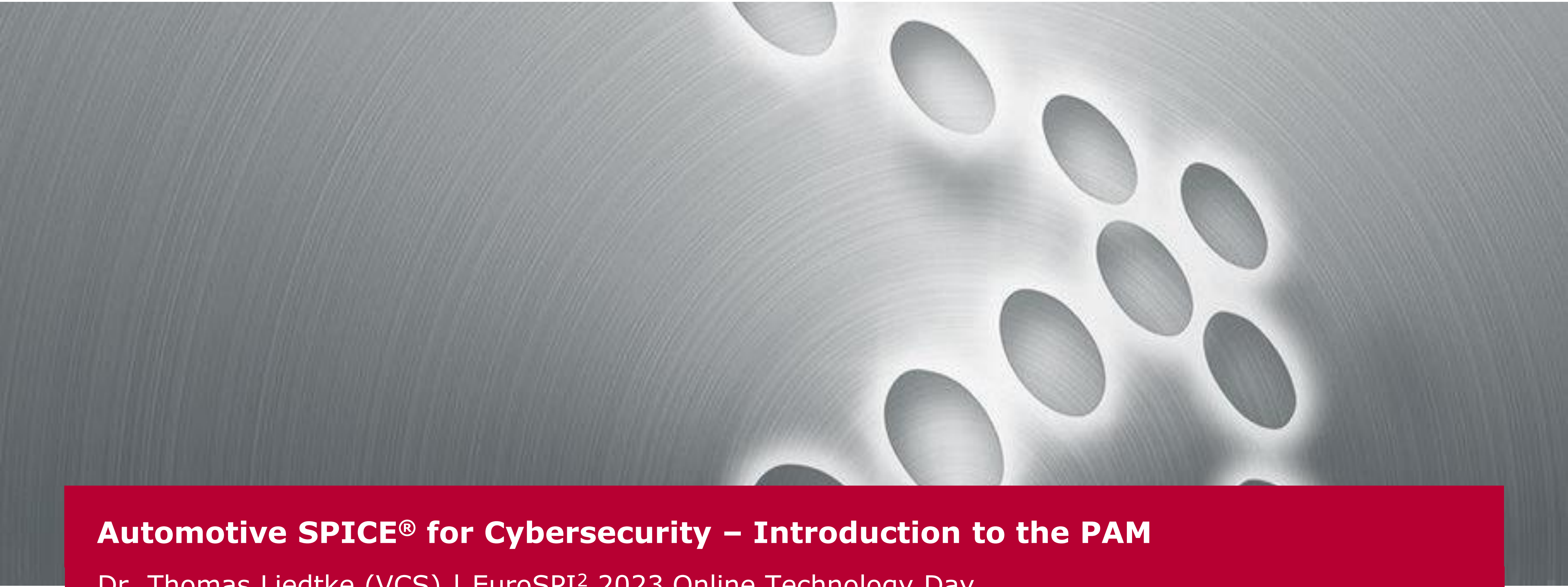
VECTOR



Automotive SPICE® for Cybersecurity – Introduction to the PAM

Dr. Thomas Liedtke (VCS) | EuroSPI² 2023 Online Technology Day

V1.0 | 2023-08-27

Introduction - Motivation

Dr. Thomas Liedtke

Experiences:

- Cybersecurity, Functional Safety, Automotive SPICE®, Privacy, Project Management
- Implementation of Security MS
- Process Improvement, Risk Management
- Functional Safety Manager, Cybersecurity Manager

Qualifications:

- Intacs certified Provisional Assessor Automotive SPICE®
- Trainer for TÜV NORD-QUALIFIED SECURITY ENGINEER (AUTOMOTIVE)
- ICO AMS 19011:2018 PROFESSIONAL
- ICO ISMS FOUNDATION according to TISAX
- ICO ISMS Auditor according to ISO/IEC 27001:2013
- UL-CSSP Certified Cybersecurity Professional Automotive
- Privacy Commissioner (FFD cert.)
- Information Security Commissioner (bitcom cert.)
- Professional SCRUM Master (scrum.org)

Professional career:

- PhD Computer Science/ Mathematics University of Stuttgart
- 1993 – 2007 Alcatel•Lucent, several positions
- 2007 – 2017 ICS AG, Head of Business Unit R&D
- 2017 – 2023 Kugler Maag Cie GmbH, Principal Consultant
- 2023 – today Vector Consulting Services, Manager Consulting

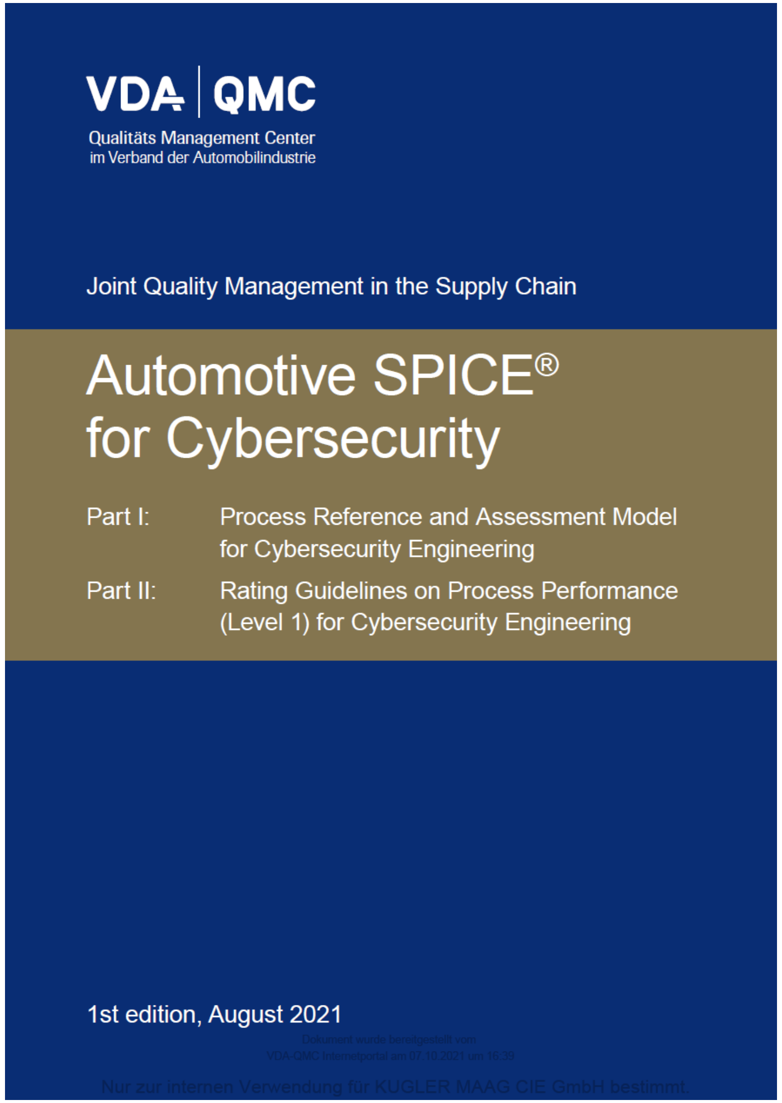
Committees:

- VDA Cybersecurity
  DIN NA052-00-32-11AK (ISO TC22/SC32/WG11)
- Member advisory board intacs
- Leader Working Group Cybersecurity SPICE intacs®
- Leader ZVEI Automotive Cybersecurity
- GI working group Privacy by Design

Table of Content

- Automotive SPICE® for Cybersecurity
- Aspects of the ISO/SAE 21434 in the scope of Automotive SPICE® for Cybersecurity
- Assessment Types
- Automotive SPICE® and Automotive SPICE® for Cybersecurity Process Reference Model
- Overview SEC-PAM
- ISO/SAE 21434 TARA – Mapping to Automotive SPICE® MAN.7-BPs
- When is an Automotive SPICE® for Cybersecurity Assessment necessary?

Automotive SPICE® for Cybersecurity – PAM 1.0



VDA | QMC
Qualitäts Management Center
im Verband der Automobilindustrie

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

1st edition, August 2021

Download: Automotive SPICE® | Home

Working Group „Cybersecurity SPICE“: Working Group "Cybersecurity SPICE" – intacs.info

122 pages

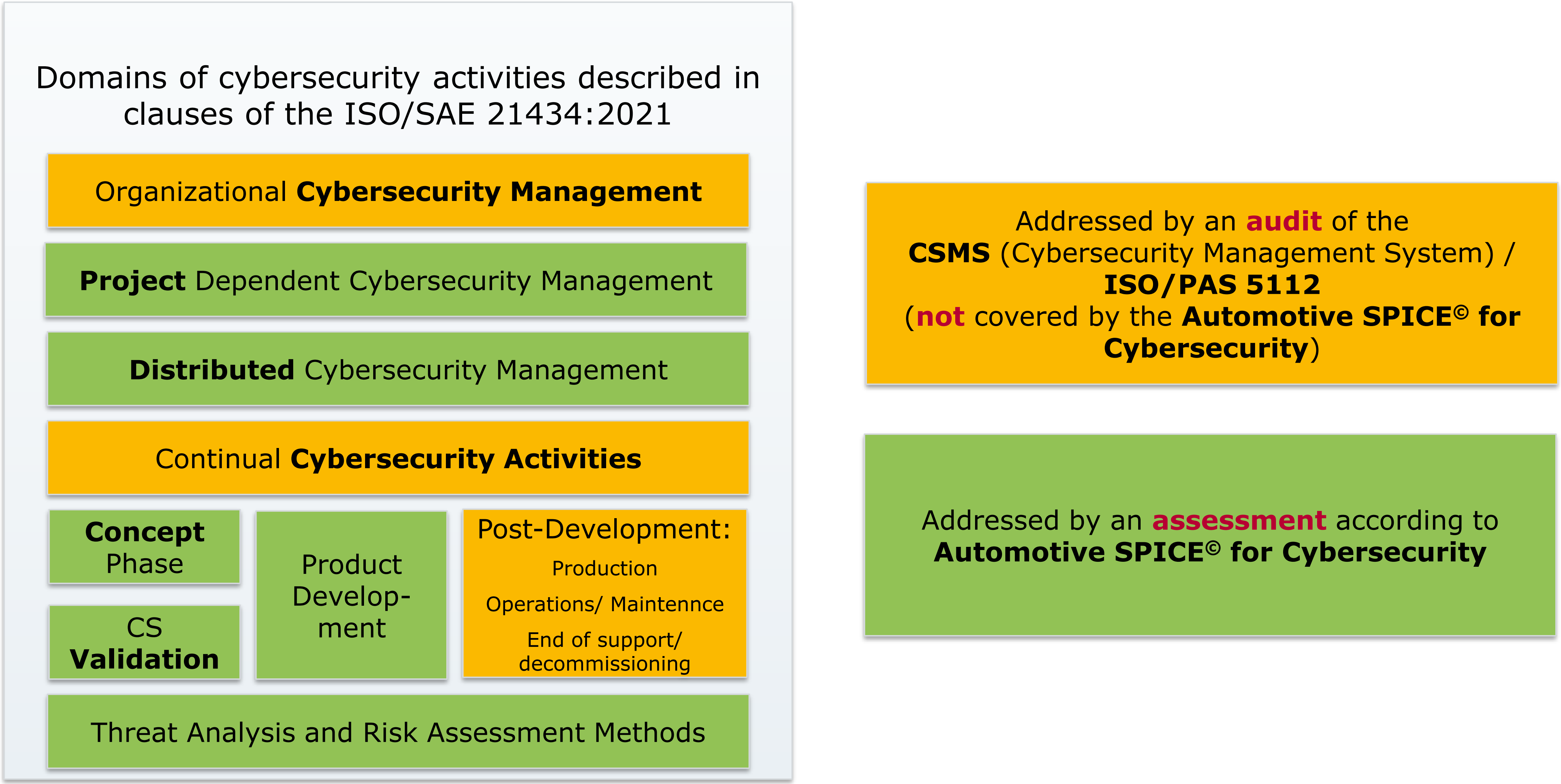
- identify systematic weaknesses in the primary lifecycle processes, management processes, and supp
- Certain aspects of the ISO/SAE 21434 are not in the scope of this document (s. slides below)

Topcis addressed

- 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.
  - Specific cybersecurity requirements relevant to the engineering activities along the whole product lifecycle
  - Basic risk methodology for road vehicle cybersecurity
  - Organization of work (planning, tailoring, responsibilities,..)

- indications in the direction of homologation are to be assessed critically.
  - Meaning of reference implementation of CSMS
  - Selected work results can be used as evidence for vehicle cybersecurity during the type approval (UNECE R.155) and re-certifications.

Aspects of the ISO/SAE 21434 in the scope of Automotive Spice® for Cybersecurity



Domains of cybersecurity activities described in clauses of the ISO/SAE 21434:2021

Organizational **Cybersecurity Management**

Project Dependent Cybersecurity Management

Distributed Cybersecurity Management

Continual **Cybersecurity Activities**

Concept Phase

CS Validation

Product Develop-ment

Post-Development:
Production
Operations/ Maintennce
End of support/ decommissioning

Threat Analysis and Risk Assessment Methods

Addressed by an **audit** of the **CSMS** (Cybersecurity Management System) / **ISO/PAS 5112** (**not** covered by the **Automotive SPICE© for Cybersecurity**)

Addressed by an **assessment** according to **Automotive SPICE© for Cybersecurity**

Project-dependent cybersecurity management

Part of add-on CS training

- Cybersecurity responsibilities: GP 2.1.5 – Define responsibilities and authorities for performing the process.
- Cybersecurity planning: GP 2.1.2 – Plan the performance of the process to fulfill the identified objectives 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 to fulfill the identified objectives.
- Reuse: included in make-buy reuse analysis SWE.2.BP6 – Evaluate alternative software architectures, SYS.3.BP5 – Evaluate alternative system architectures and REU.2 – Reuse Program Management.
- Component out of context: covered by Cybersecurity Engineering Process Group (SEC) based on assumptions regarding cybersecurity goals.
- Off-the-shelf component: ACQ.2 – Supplier Request and Selection and MAN.7 – Cybersecurity Risk Management.
- Cybersecurity case: input provided by base practices “summarize and communicate results” of engineering processes.
- Cybersecurity assessment: ASPICE for Cybersecurity is a model for process capability determination. An in-depth technical analysis is not part of an ASPICE for Cybersecurity assessment.
- Release for post-development: SPL.2 – Product Release, SUP.8 – Configuration Management Process, and SUP.1 – Quality Assurance Process.

Source: Automotive SPICE® for Cybersecurity PRM/PAM v1.0

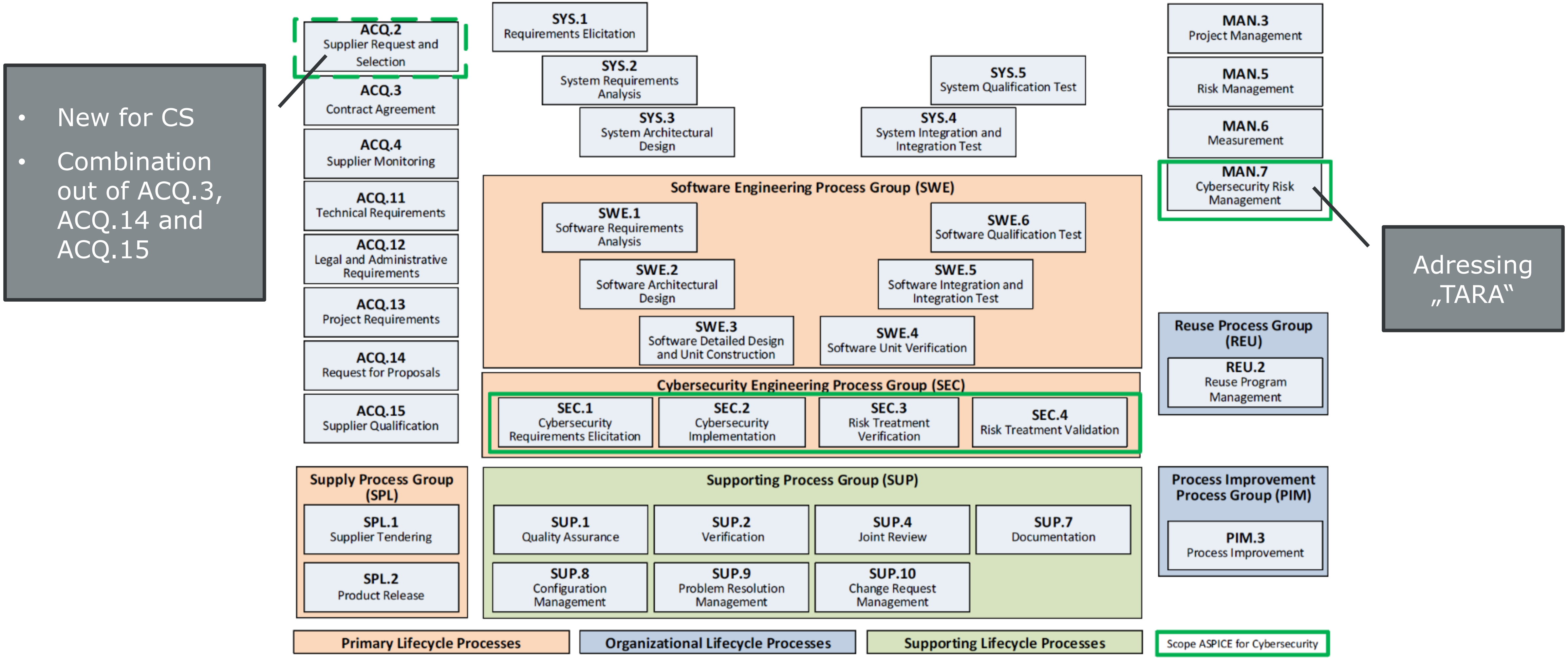
Assessment Types

Assessment Type	Recommended Assessment Scope
Combined Assessment: ▪ Assessment acc. to Automotive SPICE 3.1 PAM ▪ Assessment acc. to Automotive SPICE for Cybersecurity	▪ VDA-Scope + SEC.1-4 + MAN.7 ▪ At least one instance for ACQ.2 and ACQ.4 related to a supplier with CS relevance ▪ When assessing the Automotive SPICE 3.1 processes, the Automotive SPICE for Cybersecurity Rating Guidelines need to be applied (which is relevant for ACQ.4).
Cybersecurity Add-On Assessment: ▪ Assessment acc. to Automotive SPICE for Cybersecurity	▪ SEC.1-4 + MAN.7 + ACQ.2 ▪ ACQ.4 for an instance related to a supplier with CS relevance, and considering the Automotive SPICE for Cybersecurity Rating Guidelines ▪ SUP.1 and SUP.8 are in the target profile (see below) but can be carried over from a previous assessment.

Check also Annex D of the Automotive SPICE for Cybersecurity for assessment target profiles for type approval in the context of UNECE R155 (7.2.2.5). Automotive SPICE for Cybersecurity is not required by UNECE, but rather “cybersecurity process risk shall be managed”. The VDA created the Automotive SPICE for Cybersecurity to prove that “process-related product risk” is managed.

Source: Automotive SPICE® for Cybersecurity PRM/PAM v1.0

Automotive SPICE and Automotive SPICE for Cybersecurity Process Reference Model – Overview



- New for CS
- Combination out of ACQ.3, ACQ.14 and ACQ.15

ACQ.2 Supplier Request and Selection

ACQ.3 Contract Agreement

ACQ.4 Supplier Monitoring

ACQ.11 Technical Requirements

ACQ.12 Legal and Administrative Requirements

ACQ.13 Project Requirements

ACQ.14 Request for Proposals

ACQ.15 Supplier Qualification

SYS.1 Requirements Elicitation

SYS.2 System Requirements Analysis

SYS.3 System Architectural Design

SYS.4 System Integration and Integration Test

SYS.5 System Qualification Test

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 Integration and Integration Test

SWE.6 Software Qualification Test

Cybersecurity Engineering Process Group (SEC)

SEC.1 Cybersecurity Requirements Elicitation

SEC.2 Cybersecurity Implementation

SEC.3 Risk Treatment Verification

SEC.4 Risk Treatment Validation

MAN.3 Project Management

MAN.5 Risk Management

MAN.6 Measurement

MAN.7 Cybersecurity Risk Management

Adressing „TARA“

Reuse Process Group (REU)

REU.2 Reuse Program Management

Supply Process Group (SPL)

SPL.1 Supplier Tendering

SPL.2 Product Release

Supporting Process Group (SUP)

SUP.1 Quality Assurance

SUP.2 Verification

SUP.4 Joint Review

SUP.7 Documentation

SUP.8 Configuration Management

SUP.9 Problem Resolution Management

SUP.10 Change Request Management

Process Improvement Process Group (PIM)

PIM.3 Process Improvement

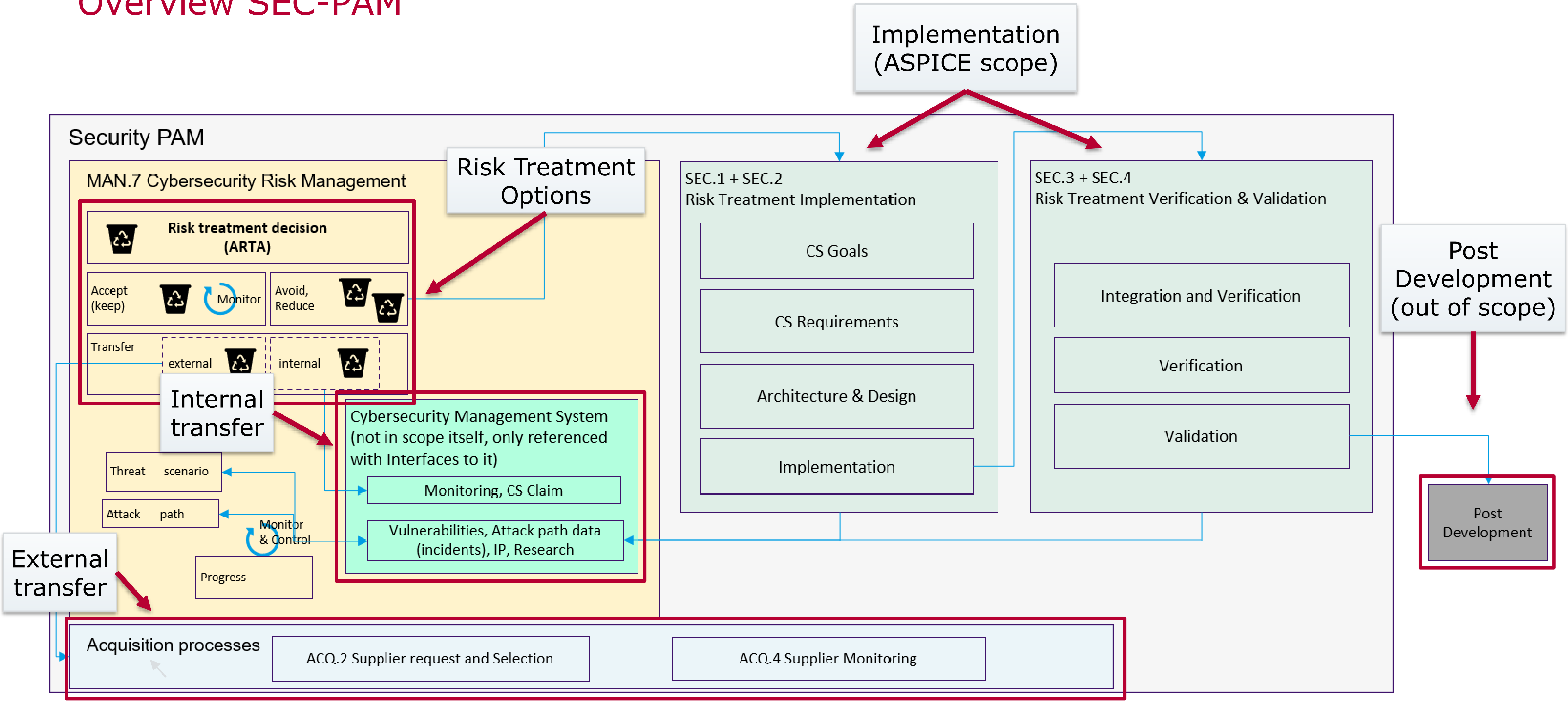
Primary Lifecycle Processes

Organizational Lifecycle Processes

Supporting Lifecycle Processes

Scope ASPICE for Cybersecurity

Overview SEC-PAM



[ASPICE-CSa]

MAN.7 Cybersecurity Risk Management

MAN.7 Cybersecurity Risk MAnagement

The purpose of the Cybersecurity Risk Management Process is to identify, **prioritize**[1], and analyze risks of damage to relevant **stakeholders**[2], and to monitor and control respective risk treatment options continuously.

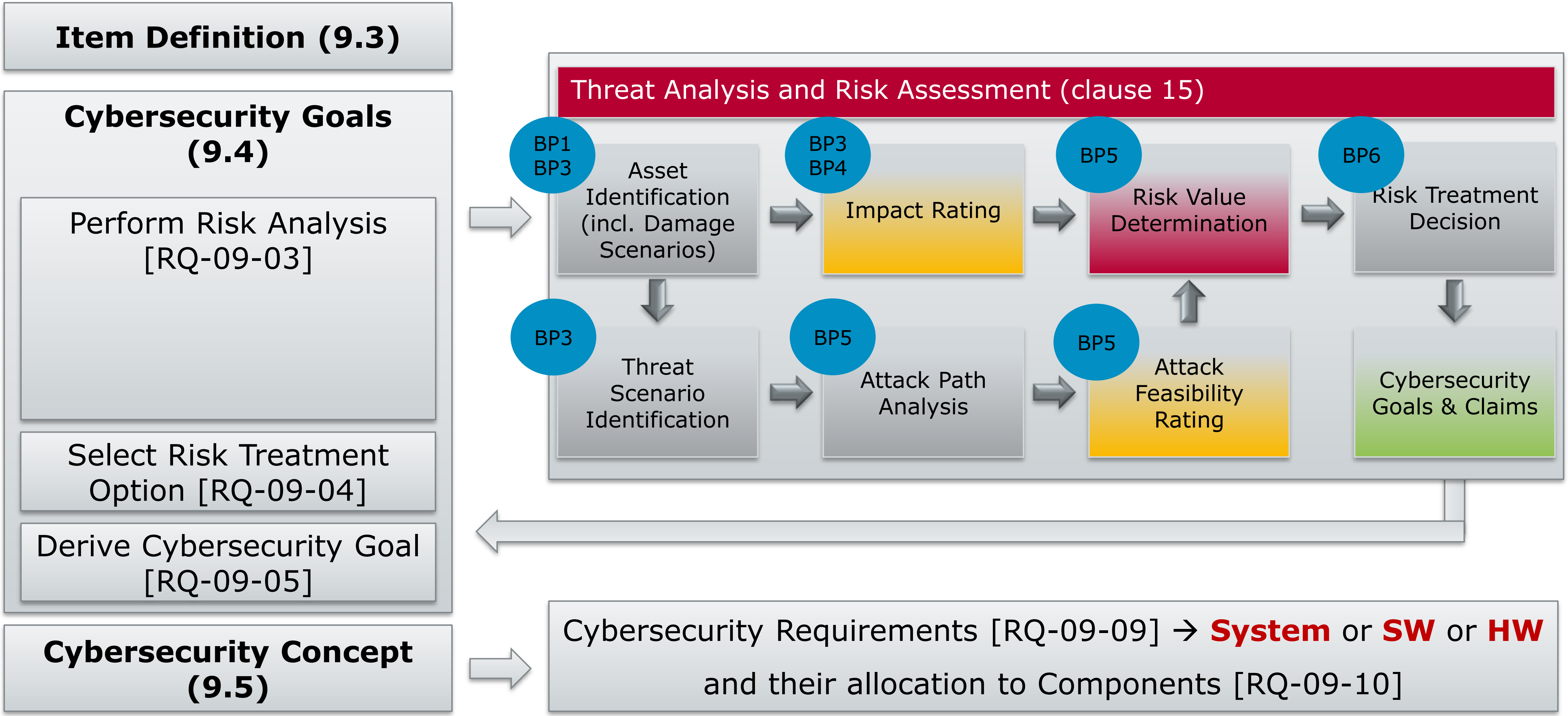
MAN.7 focuses on risks of damage to the relevant stakeholders (e.g., unauthorized disclosure of information, attacks on vehicles)

- → MAN.5 focuses on general risks in the project (resources, timing, product, quality…)
- Like MAN.5, MAN.7 is a management process:
  - Methods and process have to be defined and documented.
  - Risks have to be managed, not only analyzed.

[1] In the ISO/SAE 21434 this is called “risk value” (ISO/SAE 21434: 15.8).

[2] In the ISO/SAE 21434 stakeholders are restricted to “road users” (ISO/SAE 21434: 15.1).

Clause 15 TARA – relationship to Automotive SPICE© for Cybersecurity



Item Definition (9.3)

Cybersecurity Goals (9.4)

Perform Risk Analysis [RQ-09-03]

Select Risk Treatment Option [RQ-09-04]

Derive Cybersecurity Goal [RQ-09-05]

Cybersecurity Concept (9.5)

Threat Analysis and Risk Assessment (clause 15)

BP1 BP3 – Asset Identification (incl. Damage Scenarios)

BP3 BP4 – Impact Rating

BP5 – Risk Value Determination

BP6 – Risk Treatment Decision

BP3 – Threat Scenario Identification

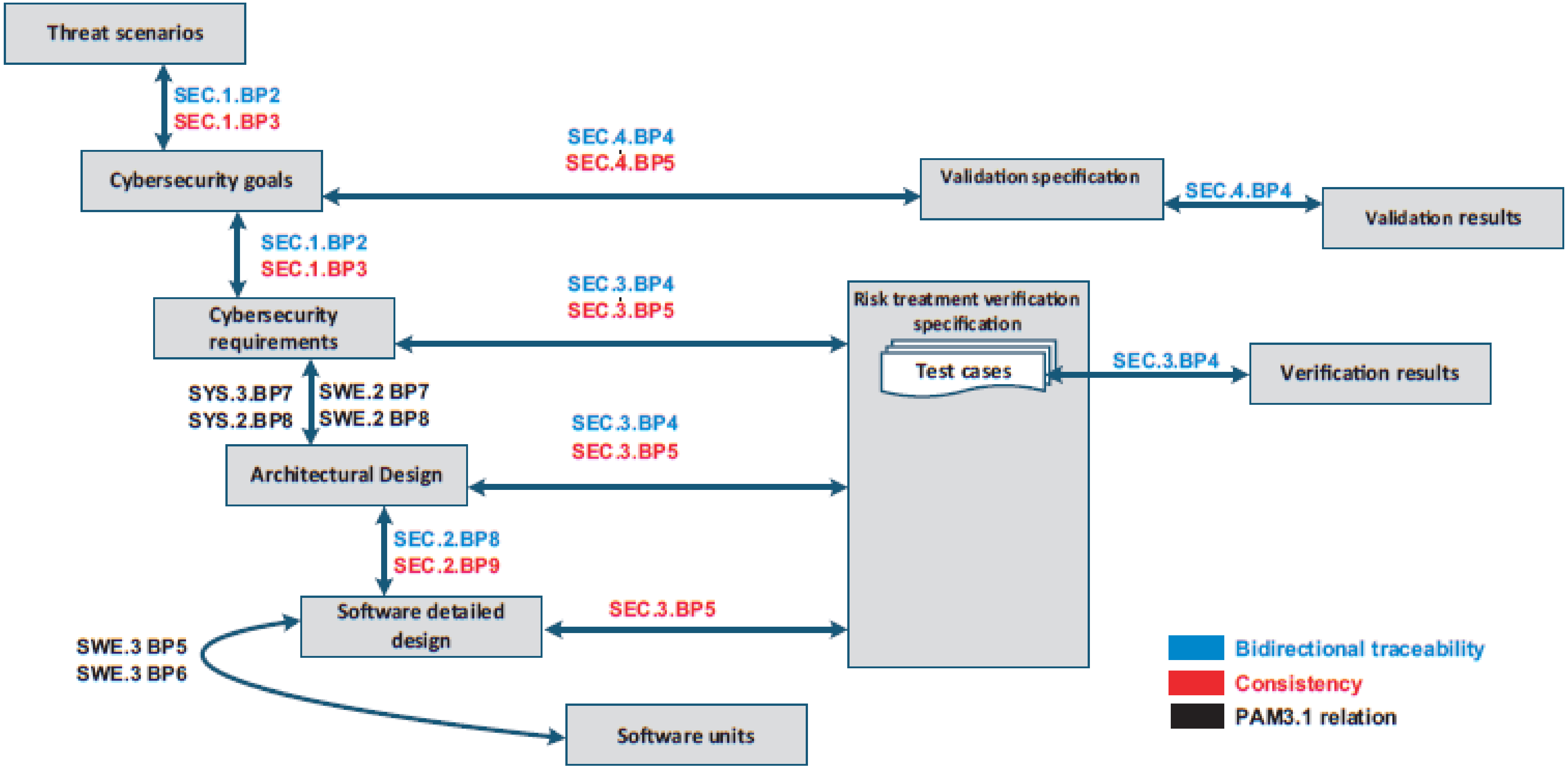
BP5 – Attack Path Analysis

BP5 – Attack Feasibility Rating

Cybersecurity Goals & Claims

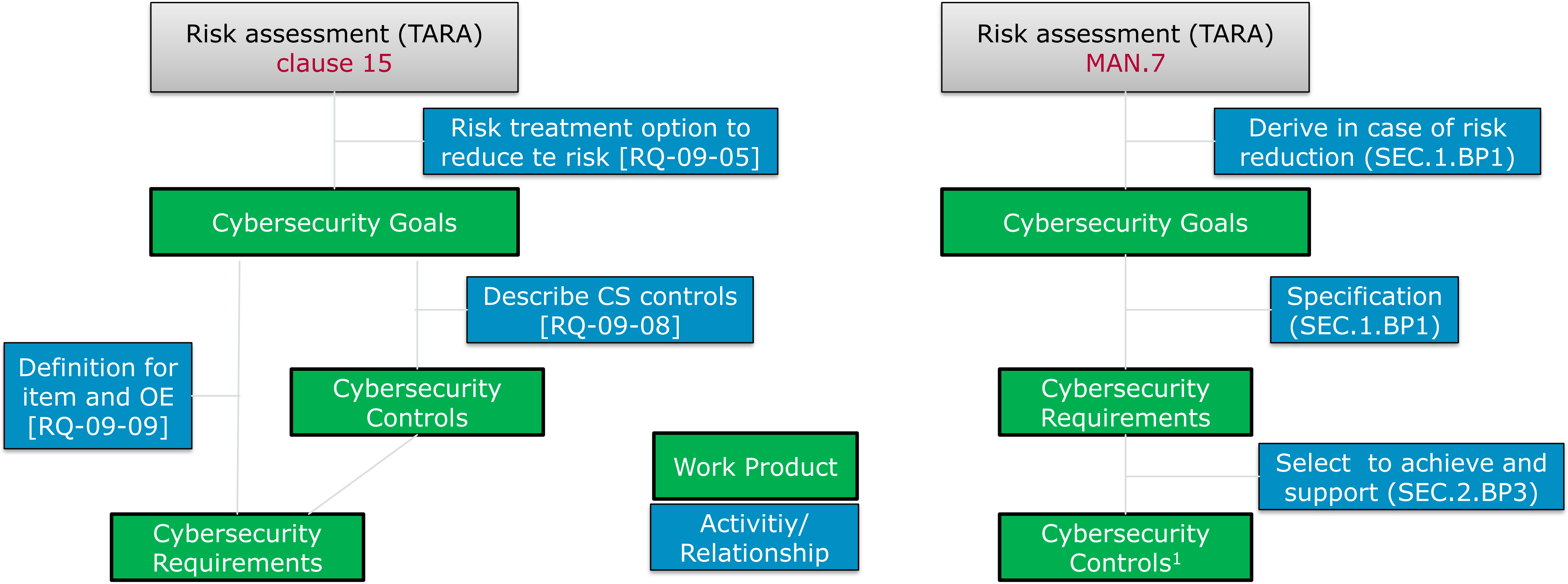
Cybersecurity Requirements [RQ-09-09] → **System** or **SW** or **HW** and their allocation to Components [RQ-09-10]

Bidirectional Traceability and Consistency



Source: Automotive SPICE® for Cybersecurity PRM/PAM v1.0

SEC.2 Differences between ISO/SAE 21434 and ASPICE for CS


Risk assessment (TARA)
clause 15
Risk treatment option to reduce te risk [RQ-09-05]
Cybersecurity Goals
Describe CS controls [RQ-09-08]
Definition for item and OE [RQ-09-09]
Cybersecurity Controls
Cybersecurity Requirements
Work Product
Activitiy/ Relationship
Risk assessment (TARA)
MAN.7
Derive in case of risk reduction (SEC.1.BP1)
Cybersecurity Goals
Specification (SEC.1.BP1)
Cybersecurity Requirements
Select to achieve and support (SEC.2.BP3)
Cybersecurity Controls[1]

3.1.14 CS Control: measure that is modifying risk

3.1.16 CS Goal: concept-level CS requirement associated with one or more threat scenarios

CS Control: is used to achieve the CS goals and CS requirements

CS Goal: Concept-level CS requirements associated with one or more threat scenarios

ACQ.x Processes

ACQ.2 Supplier Request and Selection

The purpose of the Supplier Request and Selection Process is to **award a supplier** with contract/agreement based on relevant criteria.

ACQ.4 Supplier Monitoring

The purpose of the Supplier Monitoring Process is to **track and assess the performance of the supplier** against agreed requirements.

When is an Automotive SPICE® for Cybersecurity Assessment necessary?

Recommendations from Practice:

- Customer Request (Customer specs require Automotive SPICE for Cybersecurity Assessment)
- Company cybersecurity policy
- Usefule evidences in a CSMS audit
- Pre-cybersecurity analysis check lists shows critical interfaces.
- Comparable projects showed high vulnerabilities to attacks or incidents in the past.
- Distributed development and involvement of various suppliers
  (including FOSS (Free and Open-Source Software) usage)

Recap

- Automotive SPICE for Cybersecurity
- Aspects of the ISO/SAE 21434 in the scope of Automotive Spice® for Cybersecurity
- Assessment Types
- Automotive SPICE and Automotive SPICE for Cybersecurity Process Reference Model
- Overview SEC-PAM
- ISO/SAE 21434 TARA – Mapping to Automotive SPICE© MAN.7-BPs
- When is an Automotive SPICE® for Cybersecurity Assessment necessary?

For more information about Vector
and our products please visit

www.vector.com

Passion. Partner. Value.

Vector Consulting Services

@VectorVCS

www.vector.com/consulting
consulting-info@vector.com
Phone: +49-711-80670-1520