Qualitäts Management Center
im Verband der Automobilindustrie

Automotive SPICE® for Cybersecurity

An Extension to Automotive SPICE®

Automotive SPICE® for Cybersecurity

Introduction of Speaker – Albrecht Wlokka

- Consultant @ Bosch
  - Software process improvement
  - Software quality management support and governance
  - Automotive SPICE coordination w/w (Assessments, Assessors)
  - Performing Assessments

- Experience in software domain
  - Software for quality management (1990 – 1997)
  - Quality management for software (1998 – now)
  - Automotive SPICE Competent Assessor since 2005; Principal Assessor since 2015;
  - Certified Lead Appraiser for CMMI-DEV, CMMI-SVC (2006 – 2015)
  - Certified auditor for ISO20000
  - VDA WG 13 for ASPICE (2005 – now; leader since 2019),
  - VDA WG for ISO26262 (2004-2007);
  - AutoSAR Safety Team (2005-2007);
  - VDA PG ACSMS (2018-2020)

Automotive SPICE® for Cybersecurity

Agenda

- Motivation
- Roadmap and current status
- Yellow book phase and feedback
- Content of Automotive SPICE® for Cybersecurity
- Outlook PAM4.0

Motivation

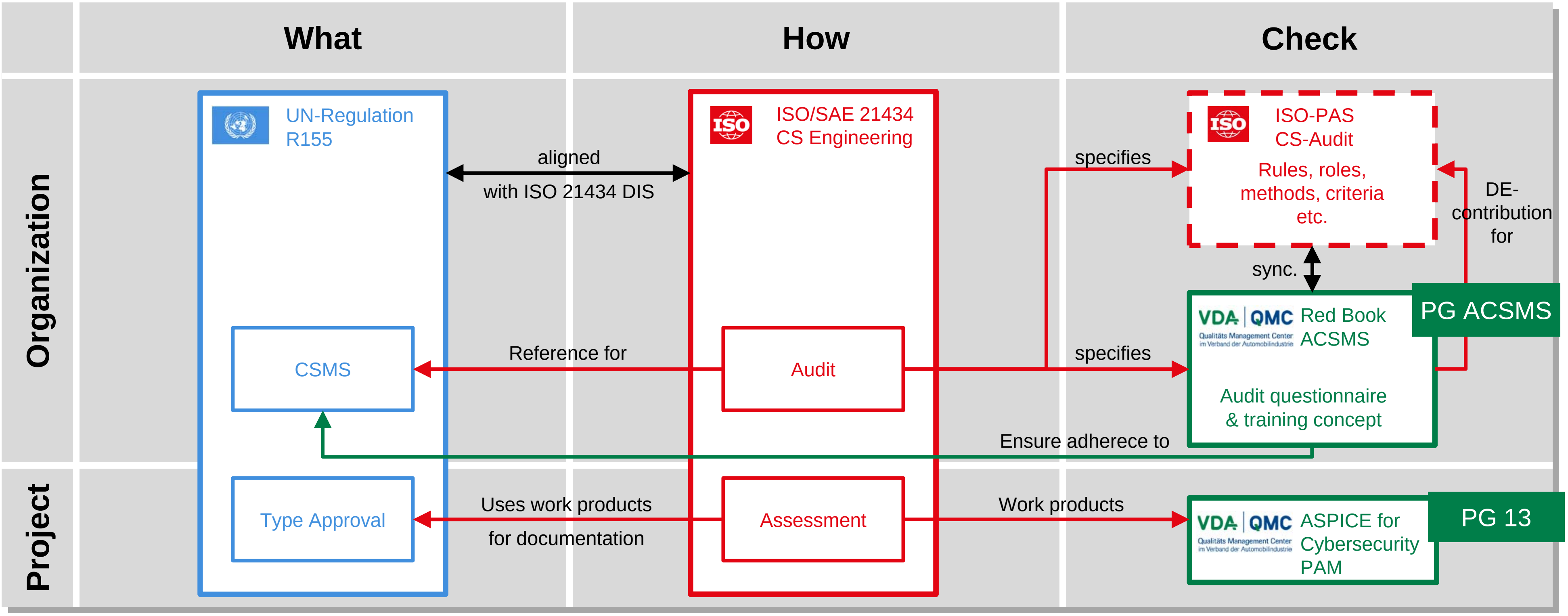
Automotive SPICE® for Cybersecurity

Motivation

- UNECE R155 Adoption for EU 07/2022 (JP 01/2022)
- Type Approval requires certified CSMS of vehicle manufacturers
- Certification of CSMS requires the management of risks related to subsidiaries and suppliers
- ASPICE is qualified to identify process related product risks
- PG13 has been authorized to
  - elaborate an enhancement to Automotive SPICE PAM3.1 to cover cybersecurity aspects
  - Develop a PAM4.0 to form an integrated framework for state-of-the-art engineering

Automotive SPICE® for Cybersecurity

Systematic of Audits and Assessments

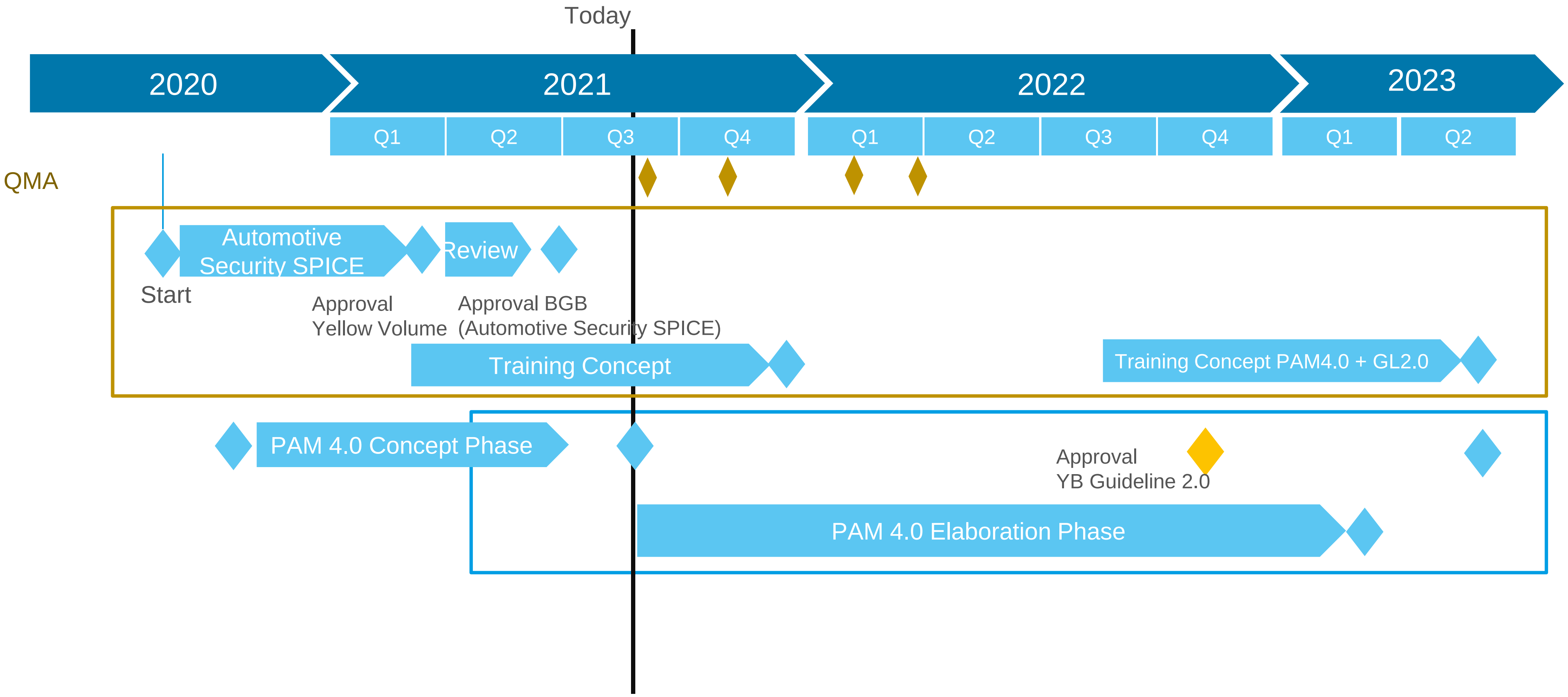


Roadmap and current Status

Automotive SPICE® for Cybersecurity

PG13 Roadmap

VDA | QMC
Qualitäts Management Center
im Verband der Automobilindustrie


Today
2020
2021
2022
2023
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
QMA
Automotive Security SPICE
Review
Start
Approval Yellow Volume
Approval BGB (Automotive Security SPICE)
Training Concept
Training Concept PAM4.0 + GL2.0
PAM 4.0 Concept Phase
Approval YB Guideline 2.0
PAM 4.0 Elaboration Phase

Yellow Book Phase and Feedback

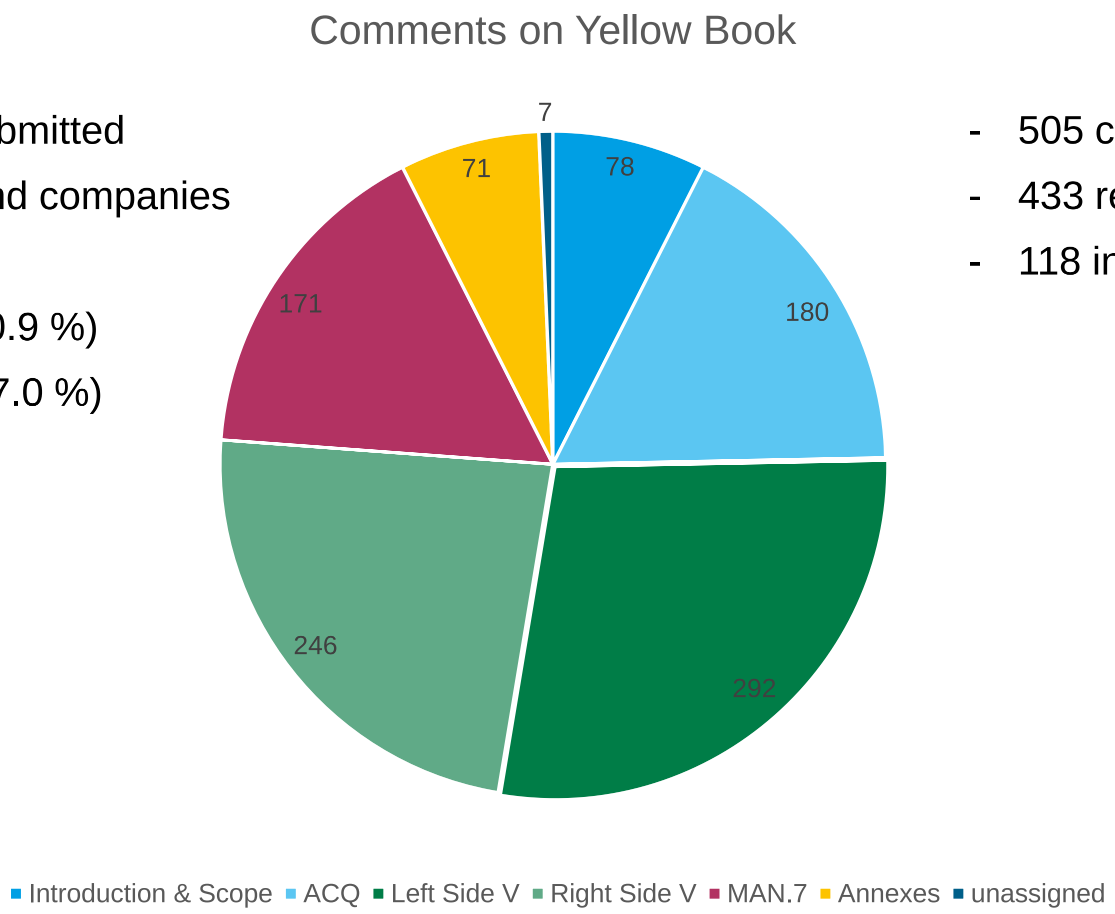
Automotive SPICE® for Cybersecurity

Feedback on Yellow Book

- 1056 comments submitted
- 27 organizations and companies

- SEC Processes (50.9 %)
- ACQ Processes (17.0 %)
- MAN.7 (16.2 %)

- Part I (66.1 %)
- Part II (27.2 %)
- Annexes (6.7 %)



- 505 comments implemented
- 433 rejected
- 118 in backlog for PAM4.0

Content of Automotive SPICE® for Cybercesurity

Automotive SPICE® for Cybersecurity

Status

Blue-Gold book is approved
BG book is in print house

Will be published as

- Free download (part I + annex A, B, C, E)
- Printed version (part I + II + annexes)
- pdf version for VDA contractors

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

Automotive SPICE® for Cybersecurity

Content of Blue-Gold Book

Part I

- Automotive SPICE® for Cybersecurity PRM and PAM with six new processes

Part II

- Guidelines for interpretation and rating of the processes of Automotive SPICE® for Cybersecurity

Annexes

- References
- Work product characteristics (for Automotive SPICE® for Cybersecurity)
- Glossary
- Target profile for type approval
- Traceability overview

Automotive SPICE® for Cybersecurity

Basic Concepts for Automotive SPICE for Cybersecurity

- Automotive SPICE PAM3.1 and Guideline remain valid; Automotive SPICE for CS is an enhancement
- Basic characteristics of ASPICE were observed (method-free, disjunctive processes, etc.)
- Automotive SPICE for CS has been developed having concepts for PAM4.0 in mind
- Structure according to Automotive SPICE 3.1 V&V (Plan, specify, perform, traceability/consistency, communicate
- No underlying customer/supplier relationship; no substructure for System/Software and Integration
- Scope can be tailored when processes do not apply
- Using Automotive SPICE for CS requires an existing assessment on VDA scope
- Development project in scope
- Minimum overlap to CSMS audit methods (VDA, ISO PAS 5112)
- Preference on generic terms versus specific ones
- Where possible, existing WPC being used (system requirements specification plus software requirements specification instead of cybersecurity requirements specification)

Automotive SPICE® for Cybersecurity

Coverage of ISO/SAE 21434

General remarks

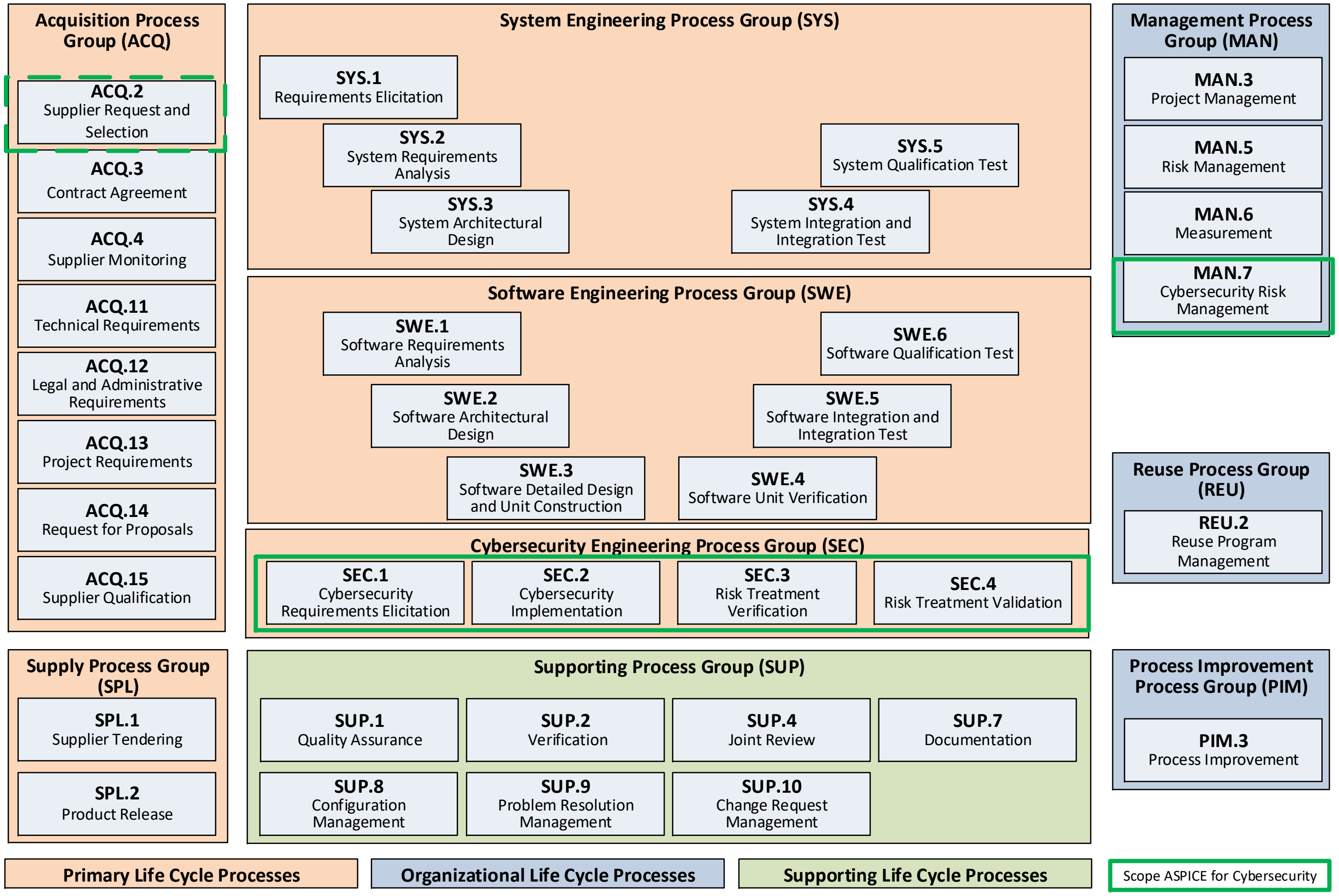
- Automotive SPICE is focused on product development, usually in a development project
- The purpose on an ASPICE Assessment for CS is to identify systematic weaknesses in primary life cycle processes, organizational life cycle processes and supporting life cycle processes
- Some aspects of ISO/SAE 21434 are evaluated on Level 2 or Level 3 and are not explicitly mentioned
- The usage of terms is wherever possible oriented on established Automotive SPICE terminology

Cybersecurity activities typically performed on organizational level and thus excluded from scope

- Organizational cybersecurity processes (chapter 5 of ISO/SAE 21434)
- Continual cybersecurity activities (chapter 8 of ISO/SAE 21434)
- Production (chapter 12 of ISO/SAE 21434)
- Operations (chapter 13 of ISO/SAE 21434)
- End of support and decommissioning (chapter 14 of ISO/SAE 21434)

Automotive SPICE® for Cybersecurity

Automotive SPICE for Cybersecurity PAM - Overview



Acquisition Process Group (ACQ)

- **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

System Engineering Process Group (SYS)

- **SYS.1** Requirements Elicitation
- **SYS.2** System Requirements Analysis
- **SYS.3** System Architectural Design
- **SYS.4** System Integration and Integration 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

Management Process Group (MAN)

- **MAN.3** Project Management
- **MAN.5** Risk Management
- **MAN.6** Measurement
- **MAN.7** Cybersecurity Risk Management

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)

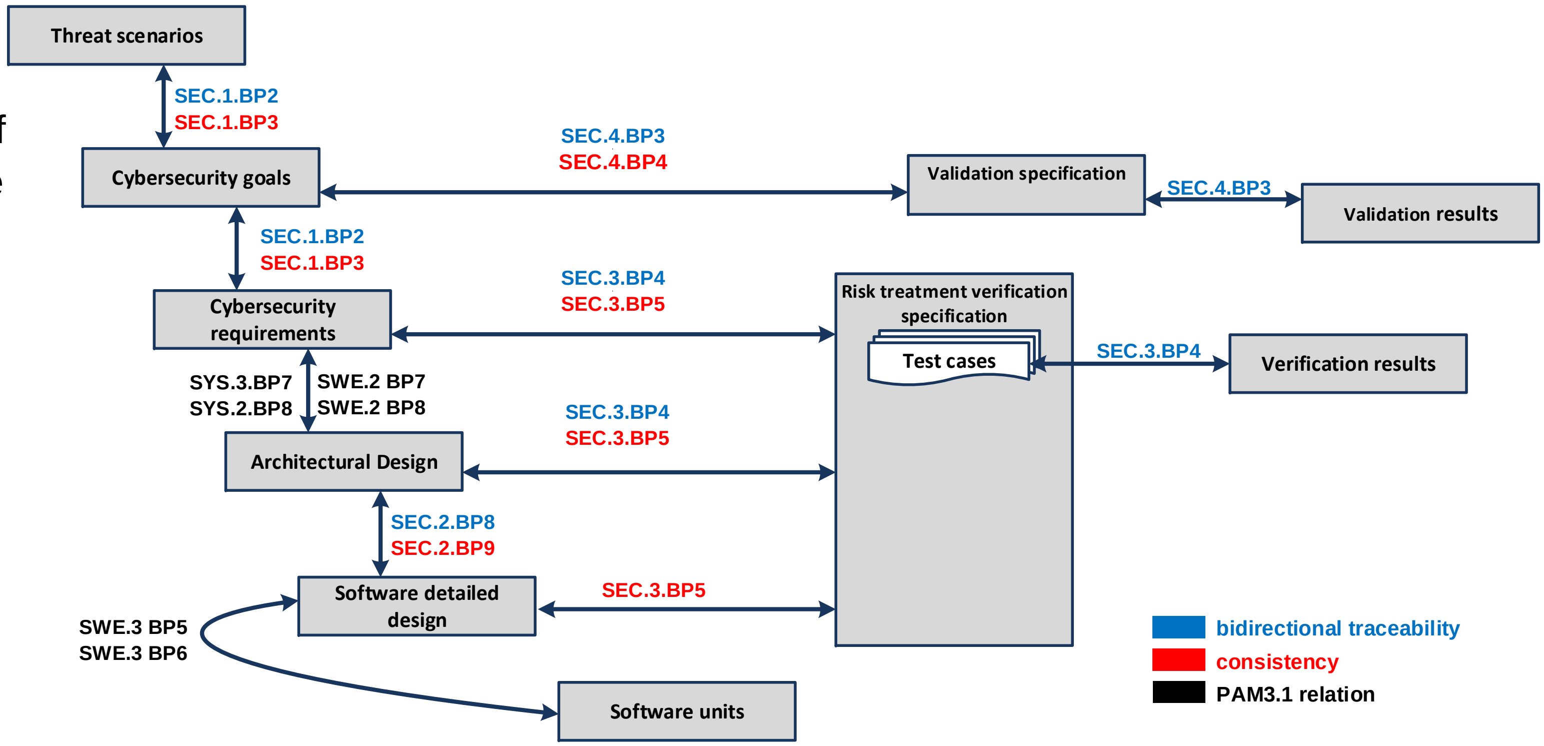
- **PIM.3** Process Improvement

Primary Life Cycle Processes | **Organizational Life Cycle Processes** | **Supporting Life Cycle Processes** | Scope ASPICE for Cybersecurity

Automotive SPICE® for Cybersecurity

Feedback on Yellow Book – Overview Traceability and Consistency

- Underlines the need of an existing VDA scope assessment
- Confirms adequacy of PAM enhancement



Threat scenarios

SEC.1.BP2
SEC.1.BP3

Cybersecurity goals

SEC.4.BP3
SEC.4.BP4

Validation specification

SEC.4.BP3

Validation results

SEC.1.BP2
SEC.1.BP3

Cybersecurity requirements

SEC.3.BP4
SEC.3.BP5

Risk treatment verification specification

Test cases

SEC.3.BP4

Verification results

SYS.3.BP7
SYS.2.BP8

SWE.2 BP7
SWE.2 BP8

Architectural Design

SEC.3.BP4
SEC.3.BP5

SEC.2.BP8
SEC.2.BP9

Software detailed design

SEC.3.BP5

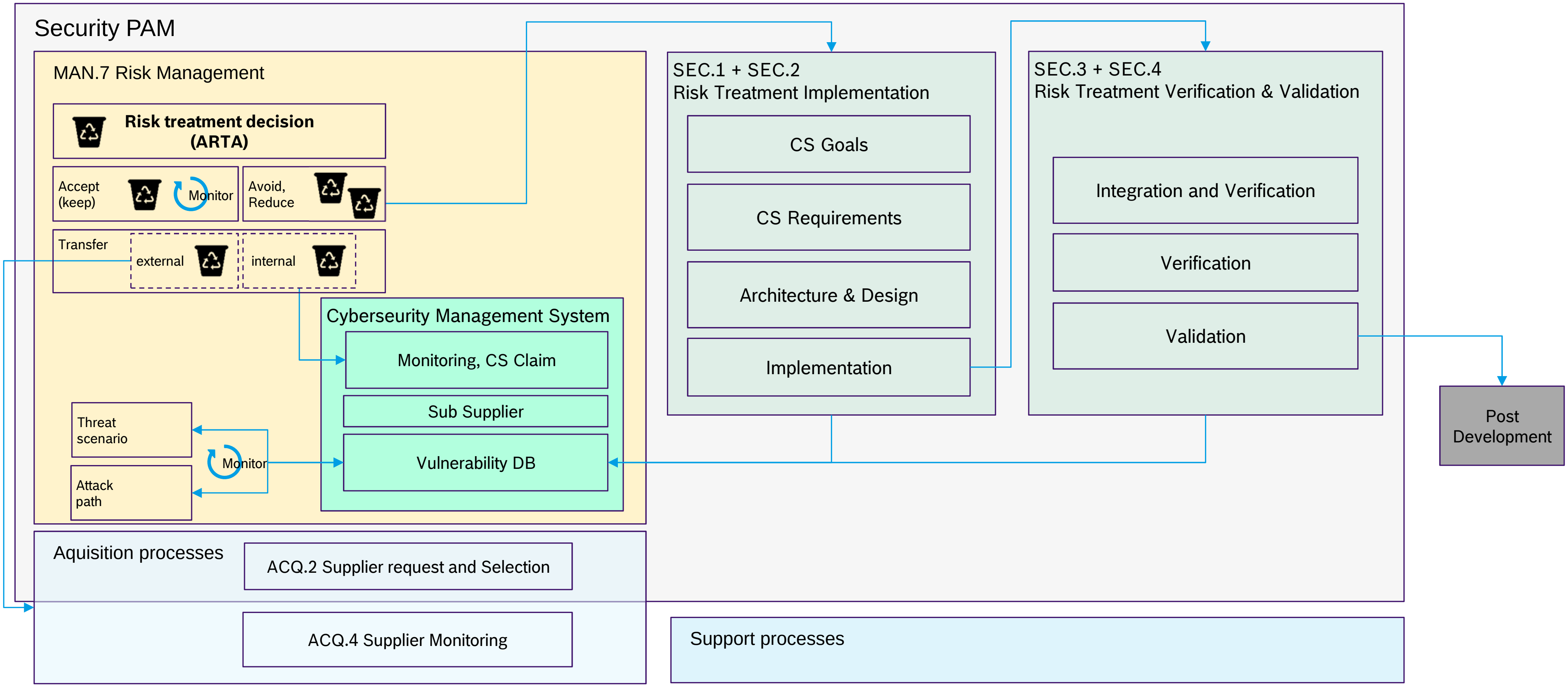
SWE.3 BP5
SWE.3 BP6

Software units

🟦 bidirectional traceability
🟥 consistency
⬛ PAM3.1 relation

Automotive SPICE® for Cybersecurity

Interaction across Processes



Automotive SPICE® for Cybersecurity

Cybersecurity Risk Management (MAN.7) - Scope

MAN.7:

- Definition of a process for cybersecurity Risk assessment
- Generalization of the process to further alignment with safety development
- No Cybersecurity specific terms.
- Covers chapter 15 and 9.3 of ISO/SAE 21434.

Automotive SPICE® for Cybersecurity

SEC.1 CS Requirements Elicitation / SEC.2 CS Implementation

SEC.1 Cybersecurity Requirements Elicitation

- Covers the elicitation of CS goals and CS requirements
- CS requirements are collected in a (system or software) requirements specification
- Covers chapter 9.4 and 9.5 of ISO/SAE 21434

SEC.2 Cybersecurity Implementation

- Covers the processing of risks that require risk mitigation (not CS claims)
- No distinction between system and software
- Covers architectural design, detailed design and implementation
- Covers identification and communication of vulnerabilities
- Covers chapter 10.4.1 of ISO/SAE 21434

Automotive SPICE® for Cybersecurity

SEC.3 Risk treatment verification / SEC.4 Risk treatment validation

SEC.3 Risk treatment verification

- Coverage of risk treatment measures
- Compliance of the implementation to the cybersecurity requirements and the architectural design
- Covers chapter 10.4.2 of ISO/SAE 21434

SEC.4 Risk treatment validation

- Compliance of the implementation to the cybersecurity goals
- Covers chapter 11 of ISO/SAE 21434

Automotive SPICE® for Cybersecurity

ACQ.2 Supplier Request and Selection

General remarks

- Consideration of requirements / recommendations and work products ISO/SAE 21434 (chapter 7)
- Implementation via changes / additions in process purpose, outcomes, base practices and output work products

ACQ.2 Supplier Request and Selection

- Relevant CS aspects of former non VDA scope processes ACQ.3 (Contract Agreement), ACQ.14 (Request for proposals) and ACQ.15 (Supplier Qualification) combined into new process ACQ.2
- Focus on supplier evaluation, selection and contractual agreement of CS specific aspects
- Renamed output work product „12-01 Request for proposal“ to „12-01 Request for quote“

Automotive SPICE® for Cybersecurity

Target Profile for Type Approval

Rationale

- Focus is on the fulfillment of the process purpose

Processes PAM3.1	Passed	Passed with Conditions
ACQ.4 Supplier Monitoring	F	L
SYS.2 System Requirements Analysis	F	L
SYS.3 System Architectural Design	F	L
SYS.4 System Integration and Integration Test	F	L
SYS.5 System Qualification Test	F	L
SWE.1 Software Requirements Analysis	F	L
SWE.2 Software Architectural Design	F	L
SWE.3 Software Detailed Design and Unit Construction	F	L
SWE.4 Software Unit Verification	F	L
SWE.5 Software Integration and Integration Test	F	L
SWE.6 Software Qualification Test	F	L
SUP.1 Quality Assurance	L	L
SUP.8 Configuration Management	L	L
SUP.9 Problem Resolution Management	F	L
SUP.10 Change Request Management	F	L
MAN.3 Project Management	L	L

Processes Automotive SPICE for Cybersecurity	Passed	Passed with Conditions
ACQ.2 Supplier request and selection	F	L
ACQ.4 Supplier Monitoring	F	L
SEC.1 Cybersecurity Requirements Elicitation	F	L
SEC.2 Cybersecurity Implementation	F	L
SEC.3 Risk Treatment Verification	F	L
SEC.4 Risk Treatment Validation	F	L
MAN.7 Project Management	F	L
SUP.1 Quality Assurance	F	L
SUP.8 Configuration Management	F	L

Outlook to PAM4.0

Automotive SPICE® for Cybersecurity

A view to PAM4.0

Goals

- Clear distinction of basic requirements versus capability dimension
- Provide flexibility to cover common use cases
- Reduce assessment duration
- Eliminate redundancies

Challenges

- The question of measurement framework (PAM3.1; ISO33020:2019; proprietary)
- Level of abstraction (generic or specific)
- How to include state-of-the-art methods and processes (AI, Continuous development)

Automotive SPICE® for Cybersecurity

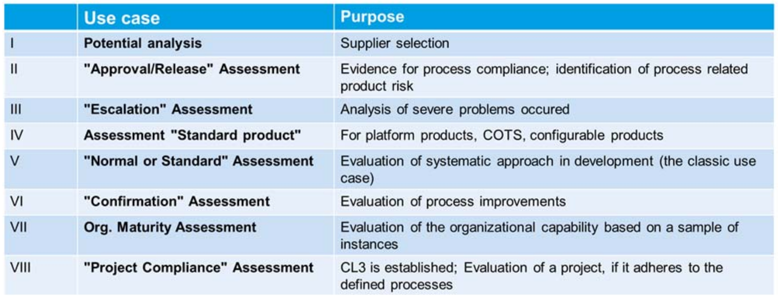
A view to PAM4.0 – Use Cases

	Use case	Purpose
I	**Potential analysis**	Supplier selection
II	**"Approval/Release" Assessment**	Evidence for process compliance; identification of process related product risk
III	**"Escalation" Assessment**	Analysis of severe problems occured
IV	**Assessment "Standard product"**	For platform products, COTS, configurable products
V	**"Normal or Standard" Assessment**	Evaluation of systematic approach in development (the classic use case)
VI	**"Confirmation" Assessment**	Evaluation of process improvements
VII	**Org. Maturity Assessment**	Evaluation of the organizational capability based on a sample of instances
VIII	**"Project Compliance" Assessment**	CL3 is established; Evaluation of a project, if it adheres to the defined processes

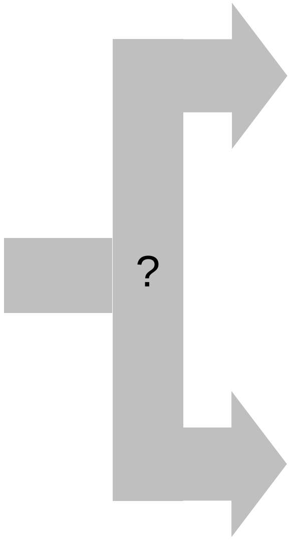
Automotive SPICE® for Cybersecurity

How many PRMs do we need

VDA | QMC
Qualitäts Management Center
im Verband der Automobilindustrie



	Use case	Purpose
I	**Potential analysis**	Supplier selection
II	**"Approval/Release" Assessment**	Evidence for process compliance; identification of process related product risk
III	**"Escalation" Assessment**	Analysis of severe problems occured
IV	**Assessment "Standard product"**	For platform products, COTS, configurable products
V	**"Normal or Standard" Assessment**	Evaluation of systematic approach in development (the classic use case)
VI	**"Confirmation" Assessment**	Evaluation of process improvements
VII	**Org. Maturity Assessment**	Evaluation of the organizational capability based on a sample of instances
VIII	**"Project Compliance" Assessment**	CL3 is established; Evaluation of a project, if it adheres to the defined processes



Scenario A –
one PRM with one PAM for all use cases

Scenario B –
one PRM with multiple PAMs for use cases

Scenario C – different PRMs

- **E.g. Improvement Assessment:**
  - Full PRM

- **E.g. Potential Analysis does not need**
  - *“Traceability“*
  - *“Communicate to..“*

Automotive SPICE® for Cybersecurity

A view to PAM4.0

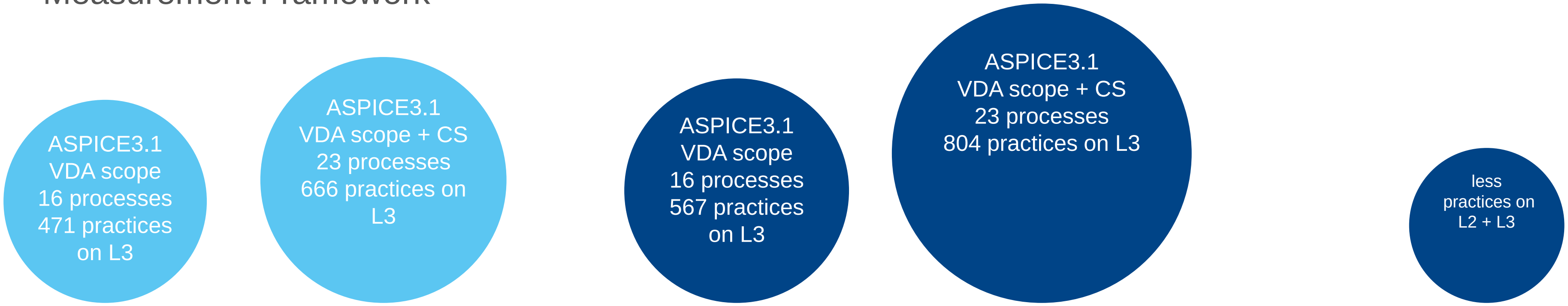
Problem

- Additional domains to evaluate state-of-the-art development (SEC, MEE, HWE, Safety, Agile, ML)
- More processes to best cover use cases
- More GP to evaluate
- Using the measurement framework of ISO33020:2019 increases the number of GP

PAM3.1
Measurement Framework

ISO33020:2019
Measurement Framework

New Idea:



ASPICE3.1
VDA scope
16 processes
471 practices
on L3

ASPICE3.1
VDA scope + CS
23 processes
666 practices on
L3

ASPICE3.1
VDA scope
16 processes
567 practices
on L3

ASPICE3.1
VDA scope + CS
23 processes
804 practices on L3

less
practices on
L2 + L3

Automotive SPICE® for Cybersecurity

A view to PAM4.0 – Further ideas

Removal of redundancies (examples)

- Traceability on level 1 and GP2.2.2
- Communicate on level 1 and GP2.1.7

Clear separation of levels (examples)

- Move strategies to level 2
- Review for consistency on level 1 or GP2.2.4
- SUP.1 BP.3 is sometimes used for demanding "rules" at CL1, however CL1 can be achieved "somehow"

Improve Guideline (examples)

- Some assessors require metrics on level 1, some on level 2 or level 3
- Necessary rules missing for not to downrate
- Clean-up of guidelines

Automotive SPICE® for Cybersecurity

Thank You?

Questions?