SYNSPACE
experts in excellence

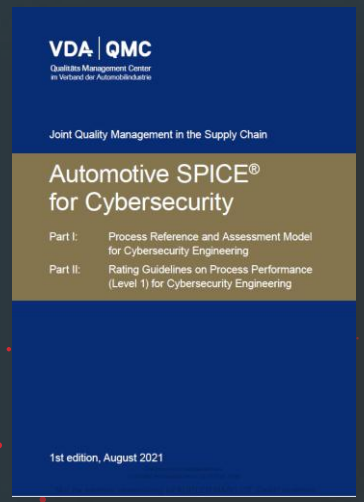
Experiences from Cybersecurity Assessments

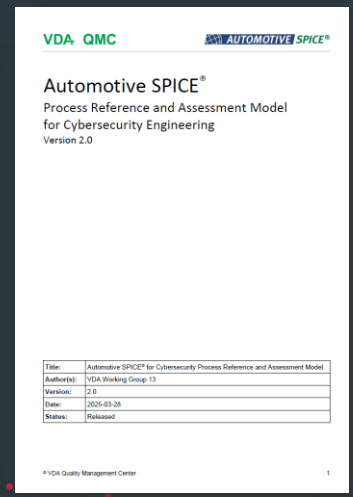
Automotive SPICE® for Cybersecurity PAM 2.0 – what are the differenes?

Intacs AT/BG/CZ/HR/HU/SI/RS Regional Event in Budapest, 14.-15.05.2025

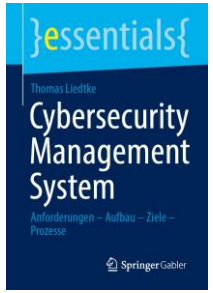
Thomas Liedtke (PhD)

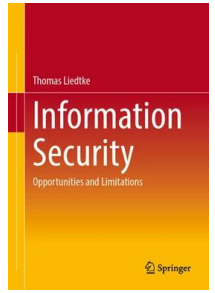
Prof. Richard Messnarz





Thomas Liedtke (PhD)





Experiences:

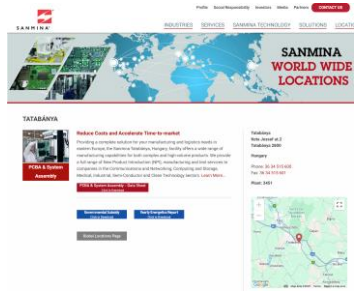
- Cybersecurity, Functional Safety, Automotive SPICE®, Privacy, Project Management
- Implementation of Security Management Systems
- Process Improvement, Risk Management
- Functional Safety Manager, Cybersecurity Manager

Qualifications:

- Trainer for SECURITY ENGINEER (AUTOMOTIVE)
- Intacs certified Provisional Assessor Automotive SPICE®
- 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 (DGI® cert.)
- Professional SCRUM Master (scrum.org)

Professional Experiences:

- Since 2025: SynSpace Group GmbH, Principal
- 2023 - 2025 Magility Cyber Security GmbH; Senior CS Expert
- 2023 – 2023 Vector Consulting Services GmbH; Manager Consultant
- 2017 – 2023 Kugler Maag Cie GmbH, Principal Consultant
- 2007 – 2017 ICS AG, Head of Business Unit R&D
- 1993 – 2007 Alcatel•Lucent, several positions
- PhD Computer Science/ Mathematics University of Stuttgart



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

Vertraulichkeitsstufe: internal

We make your improvement work

- PhD in Technical Mathematics and Informatics from TU Graz
- **Instructor Competent Level Automotive SPICE** Trainer/ Assessor
- INTACS VDA Certified **Trainer ASPICE for Cybersecurity (member of development team)**
- **VW-SQIL**
- 34 years Automotive experience
- EuroSPI/ASA (Automotive Skills Alliance) **Certified Cybersecurity Engineer/Manager Trainer**
- EuroSPI/ASA (Automotive Skills Alliance) **Certified Functional Safety Manager and Trainer**
- **ISO 26262 ASIL B, ASIL C and ASIL D project experiences** (also as Safety Manager, Safety Engineer or Assessor)
- **Experiences with cybersecurity ASPICE assessments** and cybersecurity projects / implementations
- Chair and founder of EuroSPI conferenceseries https://conference.eurospi.net/index.php/en/
- Editor of EuroSPI book series https://link.springer.com/conference/eurospi
- Moderator of SOQRATES working group of Tier 1 and OEMs – Experience exchange in ISO 26262, ISO 21434, ASPICE, and HAD vehicle topics

- Research Profile
  - **https://scholar.google.com/citations?user=v2xVlnwAAAAJ&hl=de&oi=ao**

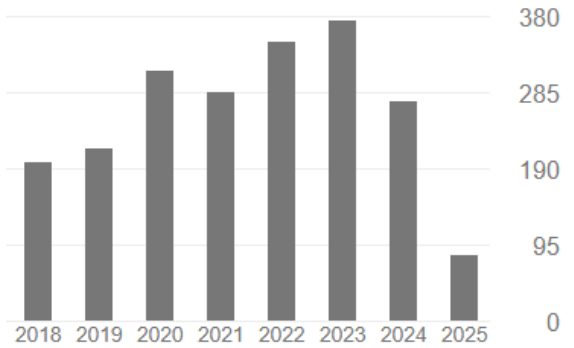
Richard Messnarz

ISCN GesmbH

Bestätigte E-Mail-Adresse bei iscn.com - Startseite

SPI Functional Safety Autom…

Cited by		VIEW ALL
	All	Since 2020
Citations	3164	1680
h-index	30	20
i10-index	92	59



Vertraulichkeitsstufe: internal

Agenda

Experiences from Cybersecurity Assessments

- Motivation
- Automotive SPICE® for Cybersecurity PAM 2.0
- Experiences from Cybersecurity Assessments
- Summary
- Bibliography

Vertraulichkeitsstufe: internal

Agenda

Experiences from Cybersecurity Assessments

- Motivation
- Automotive SPICE® for Cybersecurity PAM 2.0
- Experiences from Cybersecurity Assessments
- Summary
- Bibliography

Vertraulichkeitsstufe: internal

New version
Motivation

- Automotive SPICE® for Cybersecurity PAM 2.0 released 2025-03-28
  - Adaptations for Automotive SPICE® PAM 4.0 compliance
  - Enhancements for better alignment with ISO/SAE 21434

- Experiences we have had with cybersecurity assessments
  - Especially in conjunction with risk management

Vertraulichkeitsstufe: internal

Agenda

Experiences from Cybersecurity Assessments

- Motivation
- Automotive SPICE® for Cybersecurity PAM 2.0
- Experiences from Cybersecurity Assessments
- Summary
- Bibliography

Vertraulichkeitsstufe: internal

Adaptions to Automotive SPICE® PAM 4.0

Automotive SPICE® for Cybersecurity PAM 2.0

- Extension of Automotive SPICE® 2.0
- Work product → Information Item
- Hint to Automotive Cybersecurity Management System (ACSMS) was withdrawn → replaced by ISO/PAS 5112
- Update of references towards changed GPs of Automotive SPICE® PAM 4.0
- An in-depth technical analysis is not part of an Automotive SPICE® for Cybersecurity assessment

Vertraulichkeitsstufe: internal

Adaptions to Automotive SPICE® PAM 4.0

Automotive SPICE® for Cybersecurity PAM 2.0

- Rationale for Automotive SPICE® PAM 4.0 new process “Validation”:
  - Refers to all stakeholder goals or stakeholder requirements, not to be confused with;
  - SEC.4 focused on the cybersecurity goals (similar to CS validation (ISO/SAE 21434 cl. 9))

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

SEC.4 (Risk treatment validation process) declares that it is to confirm that the integrated system achieves the associated cybersecurity goals.

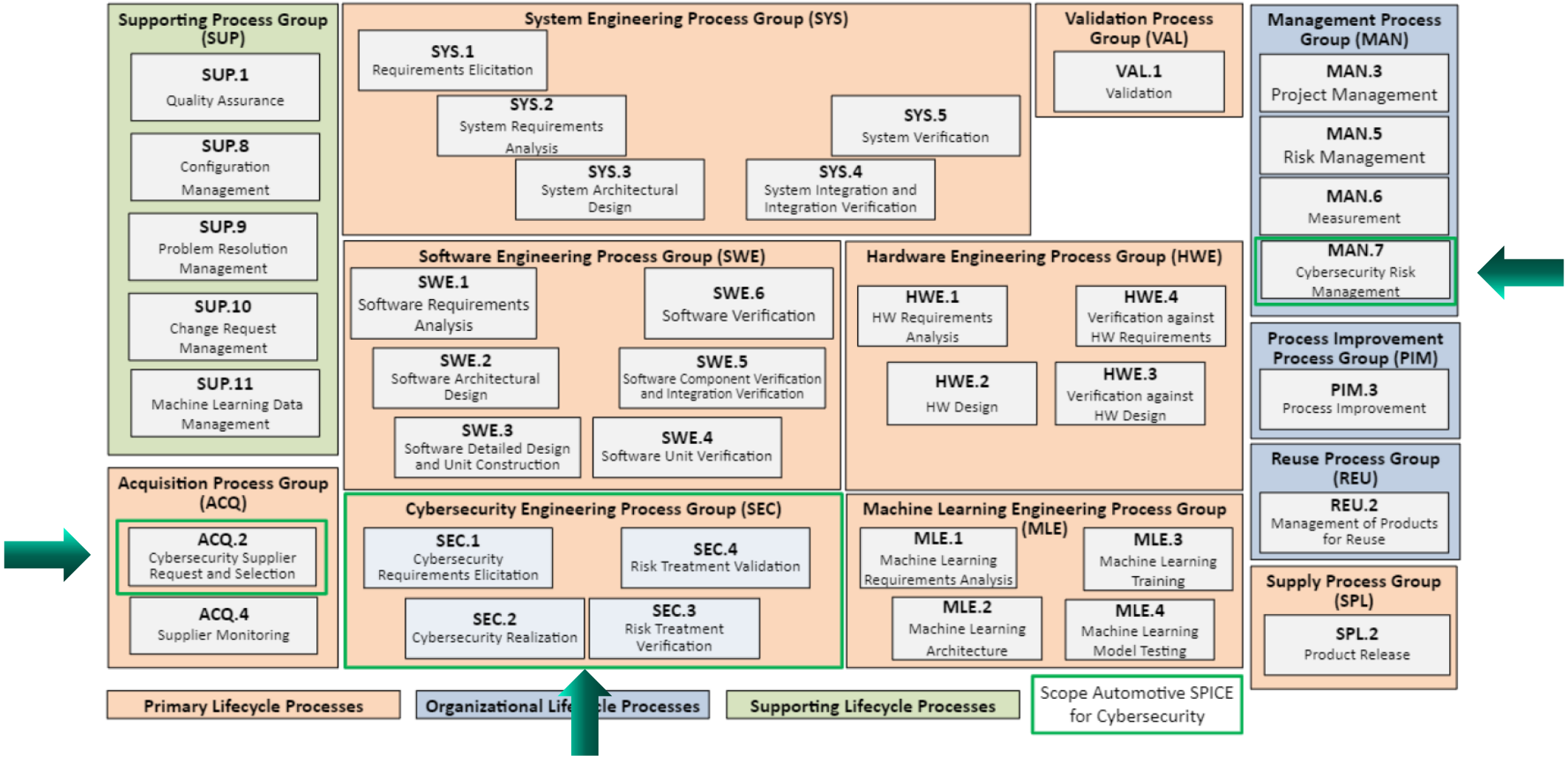
Covering unintended use

VAL.1 (Validation process) provide evidence that the delivered product satisfies the intended use expectations (stakeholder goals) in its operational target environment.

Vertraulichkeitsstufe: internal

Automotive SPICE® and Automotive SPICE® for Cybersecurity Process References Model – Overview

Automotive SPICE® for Cybersecurity PAM 2.0



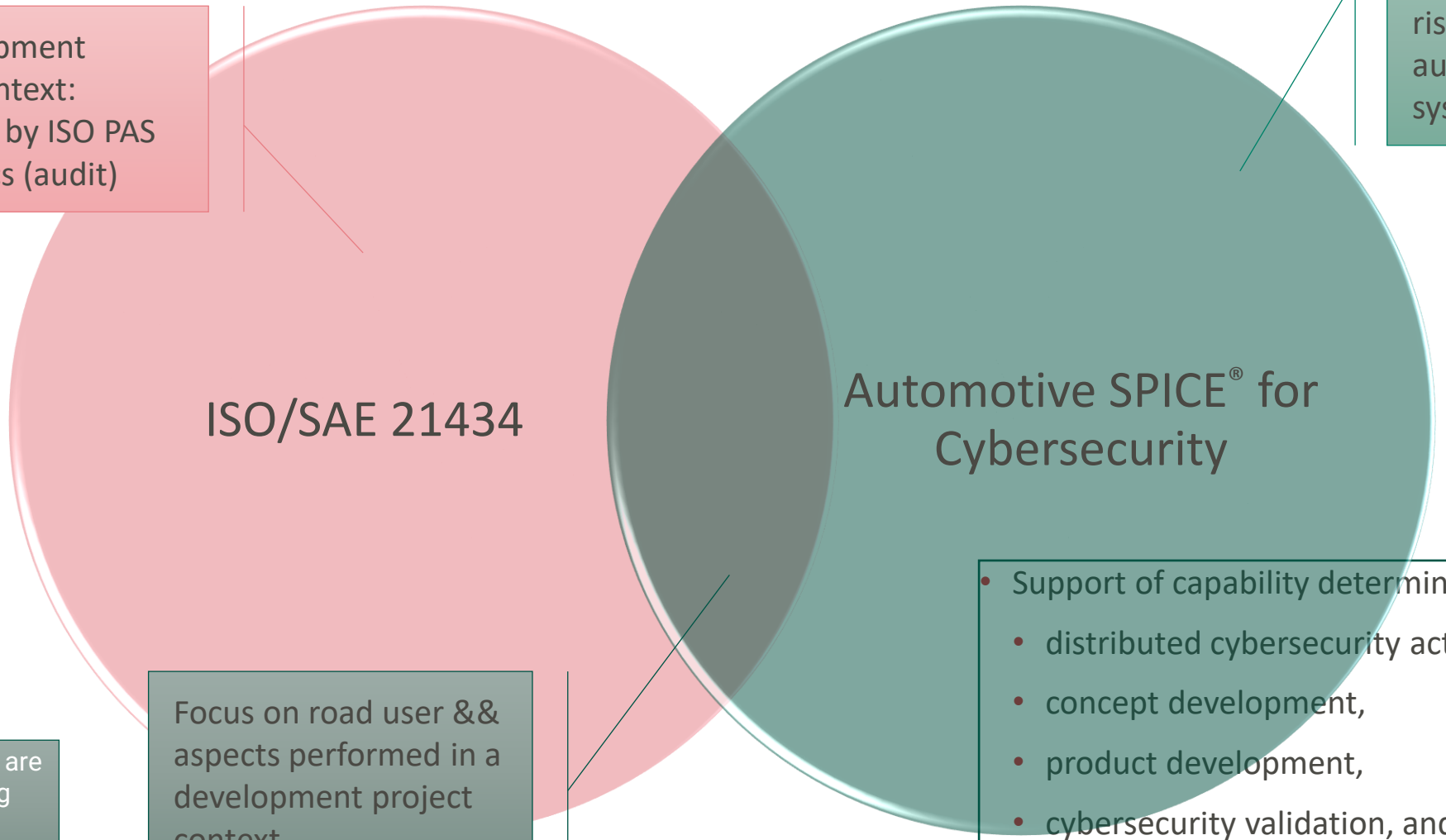
Vertraulichkeitsstufe: internal

Focus of the documents

Automotive SPICE® for Cybersecurity PAM 2.0

<> Development project context: addressed by ISO PAS 5112 topics (audit)

<> Focus road user: risks from the entire automotive eco-system



- Support of capability determination of processes for
  - distributed cybersecurity activities,
  - concept development,
  - product development,
  - cybersecurity validation, and
  - threat analysis and risk assessment

Focus on road user && aspects performed in a development project context

Size of bubbles are not representing the number of requirements

Vertraulichkeitsstufe: internal

Relation to ISO/SAE 21434

Automotive SPICE® for Cybersecurity PAM 2.0

- Automotive SPICE® for Cybersecurity assessment can identify gaps and process weaknesses in projects that are implementing cybersecurity activities.
- Valuable input for improvements of the cybersecurity processes within the organization.
- Implementing effective improvement measures derived from assessment to adjust and refine the cybersecurity management system of the organization.
- 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 Automotive SPICE® for Cybersecurity, 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.

Vertraulichkeitsstufe: internal

Changes of purpose

Automotive SPICE® for Cybersecurity PAM 2.0

PAM 1.0

- **MAN.7: Cybersecurity Risk Management**
  - Identify, prioritize, and analyze risks of damage to relevant stakeholders, and to continuously monitor and control respective risk treatment options.
- **SEC.1: Cybersecurity Requirements Elicitation**
  - Derive cybersecurity goals and requirements from the outcomes of risk management, and ensure consistency between the risk assessment, cybersecurity goals, and cybersecurity requirements.
- **SEC.2: Cybersecurity Implementation**
  - Allocate the cybersecurity requirements to the elements of the system and software and ensure they are implemented.
- **SEC.3: Risk Treatment Verification**
  - Confirm that the implementation of the design and integration of the components comply with the cybersecurity requirements, the refined architectural design, and detailed design.
- **SEC.4: Risk Treatment Validation**
  - Confirm that the integrated system achieves the associated cybersecurity goals.

PAM 2.0

- **MAN.7: Cybersecurity Risk Management**
  - The purpose is to regularly identify, analyze, prioritize, and monitor risks of damage to relevant stakeholders
- **SEC.1: Cybersecurity Requirements Elicitation**
  - The purpose is to specify cybersecurity goals and requirements from the outcomes of cybersecurity risk management covering the threat scenarios.
- **SEC.2: Cybersecurity Implementation**
  - The purpose is to refine the design of the system, software and hardware, consistent with the cybersecurity requirements and to ensure they are implemented
- **SEC.3: Risk Treatment Verification**
  - 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.
- **SEC.4: Risk Treatment Validation**
  - The purpose is to confirm that the integrated system achieves the associated cybersecurity goals.

Vertraulic

Changes Automotive SPICE® for Cybersecurity PAM 2.0 versus PAM 1.0

Automotive SPICE® for Cybersecurity PAM 2.0

- ACQ.2:
  - Contract, action, and risk mitigation plans → Commitment/ agreement, corrective actions
  - Definition of post-development phases: production, operation and decommissioning
- SEC.1:
  - Specification of cybersecurity goals instead of derivation
  - Additional hints for characteristics of requirements (e.g., verifiability)
- SEC.2:
  - Refine the design of the system, software and hardware (changed from allocation of cybersecurity requirements)
  - Vulnerabilities are analyzed → Weaknesses are analyzed
  - Risk treatment implementation → Cybersecurity implementation
  - Allocate cybersecurity requirements → Ensure consistency
  - Analyze architecture → analyze architecture for weaknesses
  - Including of HW architecture (due to Automotive SPICE® 4.0)
- SEC.3
  - Skipping BP1: Development and implementation of risk treatment verification and integration strategy
  - Add-on information item: 13-51 consistency evidence
- SEC.4
  - Skipping BP1: Development of risk treatment validation strategy
  - Skipping information item validation strategy
- Correction of terminology:
  - Probability → likelihood
  - Item definition aligned with standard

Vertraulichkeitsstufe: internal

Changes Automotive SPICE® for Cybersecurity PAM 2.0 versus PAM 1.0

Automotive SPICE® for Cybersecurity PAM 2.0

- MAN.7:
  - Add-on:
    - regularly identify, analyze, prioritize, and monitor, …
    - Item definition
    - Appropriate risk treatment is taken to mitigate … i.s.o. of risk treatment options are determined
    - Take corrective actions when risk treatment activities are not effective
    - Information Item 08-55: risk treatment
  - Skipped:
    - monitor, and control [..] risk treatment options continuously
    - SFOP as impact criteria → Risks may include the suppliers' deliverables and services.
  - Wording more in line with ISO/SAE 21434
  - Monitoring - cybersecurity information; identification of cybersecurity events – explicitly mentioned
  - Prioritize, determine the probability of occurrence → Analyze risk and determine the risk … based on impact … feasibility of an attack
  - Risk measure → Risk treatment
  - Decoupling from the "normal" risk management process

Vertraulichkeitsstufe: internal

Changes Automotive SPICE® for Cybersecurity PAM 2.0 versus PAM 1.0 – MAN.7

Automotive SPICE® for Cybersecurity PAM 2.0

PAM 1.0

- MAN.7 PAM 1.0
  - BP1: Determine cybersecurity risk management scope
  - BP2: Define cybersecurity risk management practices
  - BP3: Identify potential risks
  - BP4: Prioritize potential risks initially for damage
  - BP5: Analyze potential risks and evaluate risks
  - BP6: Define risk treatment option
  - BP7: Monitor risks
  - BP8: Take corrective action

PAM 2.0

- MAN.7 PAM 2.0
  - BP1: Identify cybersecurity risk management scope
  - BP2: Identify cybersecurity events
  - BP3: Analyze risks
  - BP4: Define risk treatment options
  - BP5: Define and perform risk treatment activities
  - BP6: Monitor risks
  - BP7: Take corrective action

Vertraulichkeitsstufe: internal

Additional information items in PAM 2.0 vs. PAM 1.0/ Automotive SPICE® 4.0

Automotive SPICE® for Cybersecurity PAM 2.0

New information items introduced with Automotive SPICE® 4.0

- 03-50: verification measures
- 04-52: hardware architecture
- 04-53: hardware detail design
- 08-55: Risk treatment
- 08-57: Validation Measure Selection Set
- 13-51: Consistency Evidence
- 13-52: Communication Evidence
- 14-02: Corrective action
- 15-51: Analysis Results
- 17-54: Requirement Attribute

Additional information items introduced with Automotive SPICE® for Cybersecurity

- 03-55: validation measures
- 17-53: Cybersecurity threat scenario

Vertraulichkeitsstufe: internal

Agenda

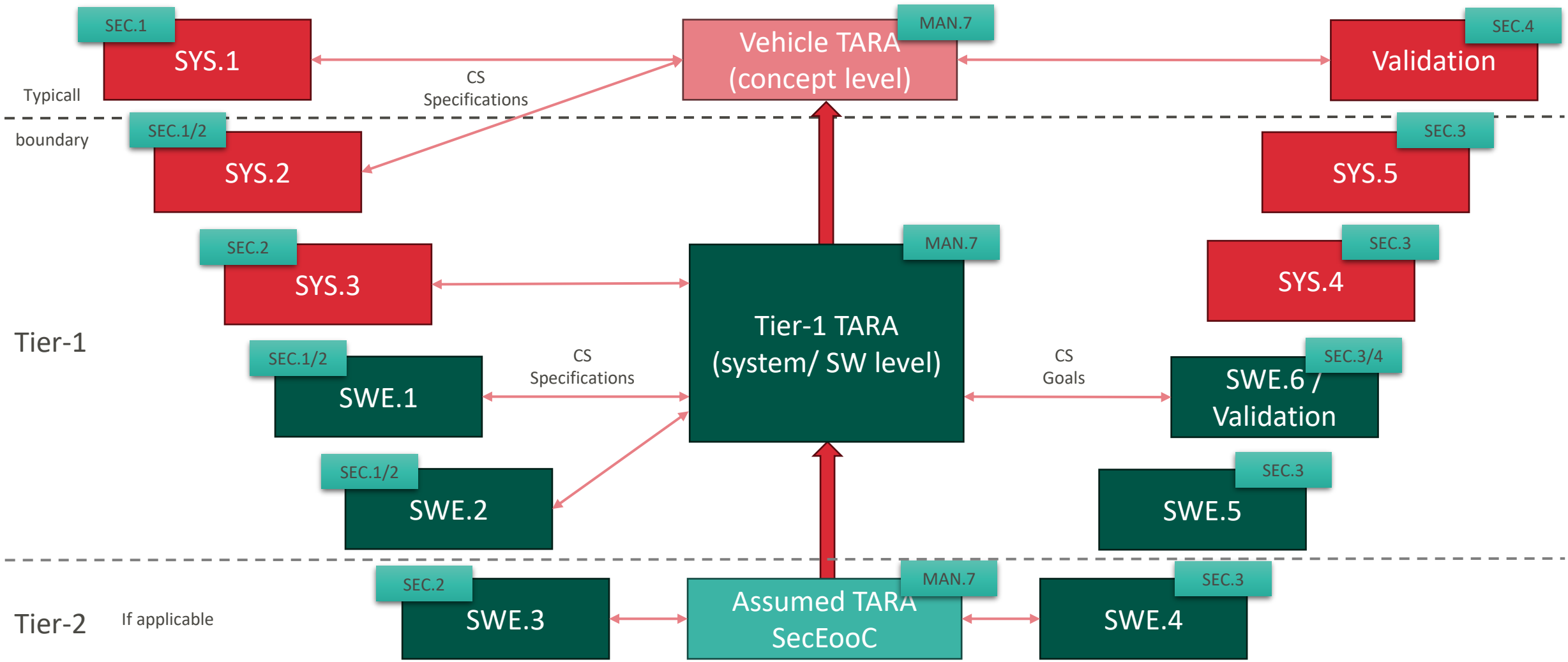
Experiences from Cybersecurity Assessments

- Motivation
- Automotive SPICE® for Cybersecurity PAM 2.0
- **Experiences from Cybersecurity Assessments**
- Summary
- Bibliography

Vertraulichkeitsstufe: internal

Risk Assessment is performed on different levels

Experiences from Cybersecurity Assessments



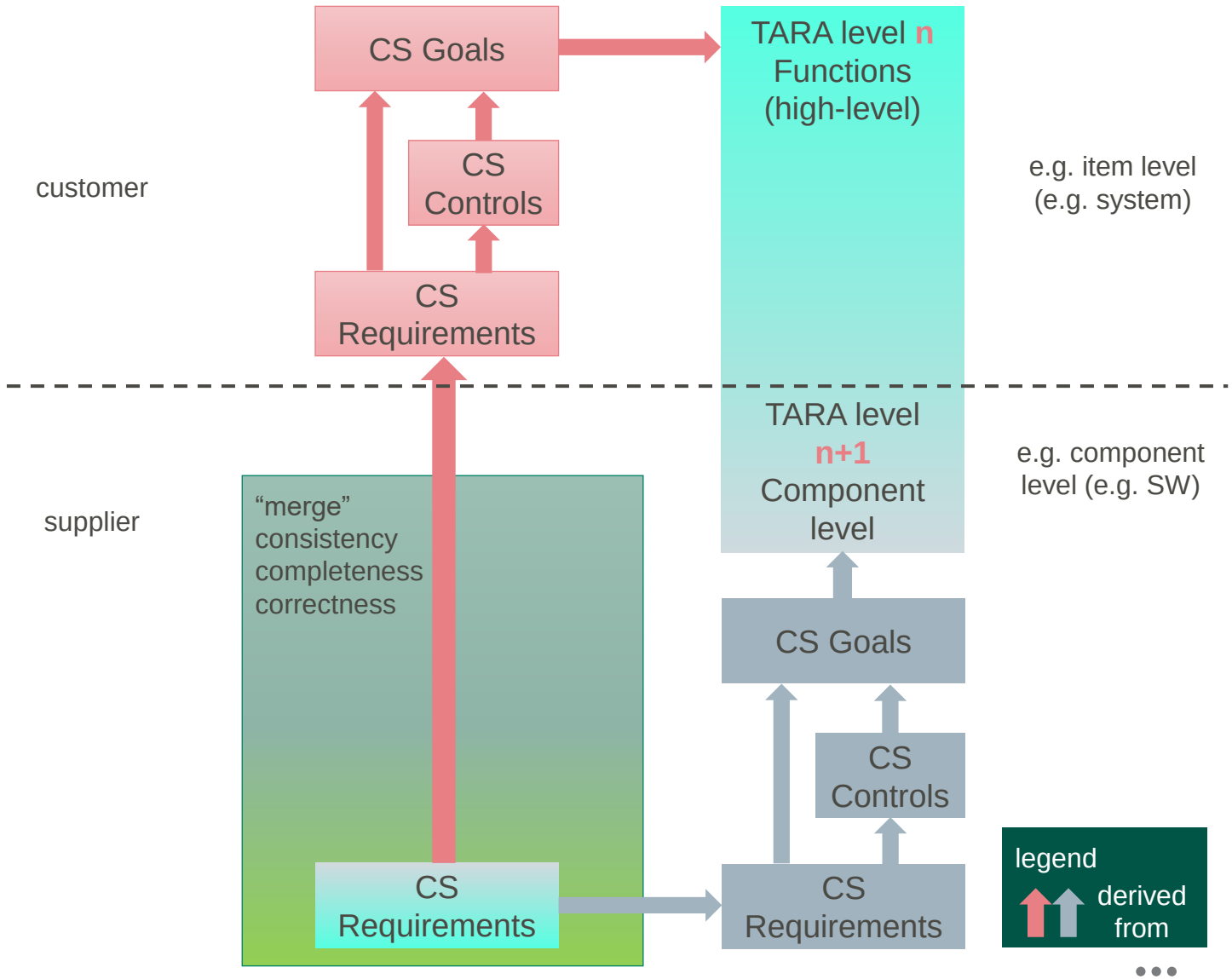
Vertraulichkeitsstufe: internal

Initial typical situation

Experiences from Cybersecurity Assessments

Typical situation:

- Multiple TARAs are created at different levels of a supply chain
- The resulting requirements need to be combined and validated as a whole
- Supplier (Tier-1, Tier-2, ...) creates its "own" TARA at its supply level for the component to be delivered (scope of supply)



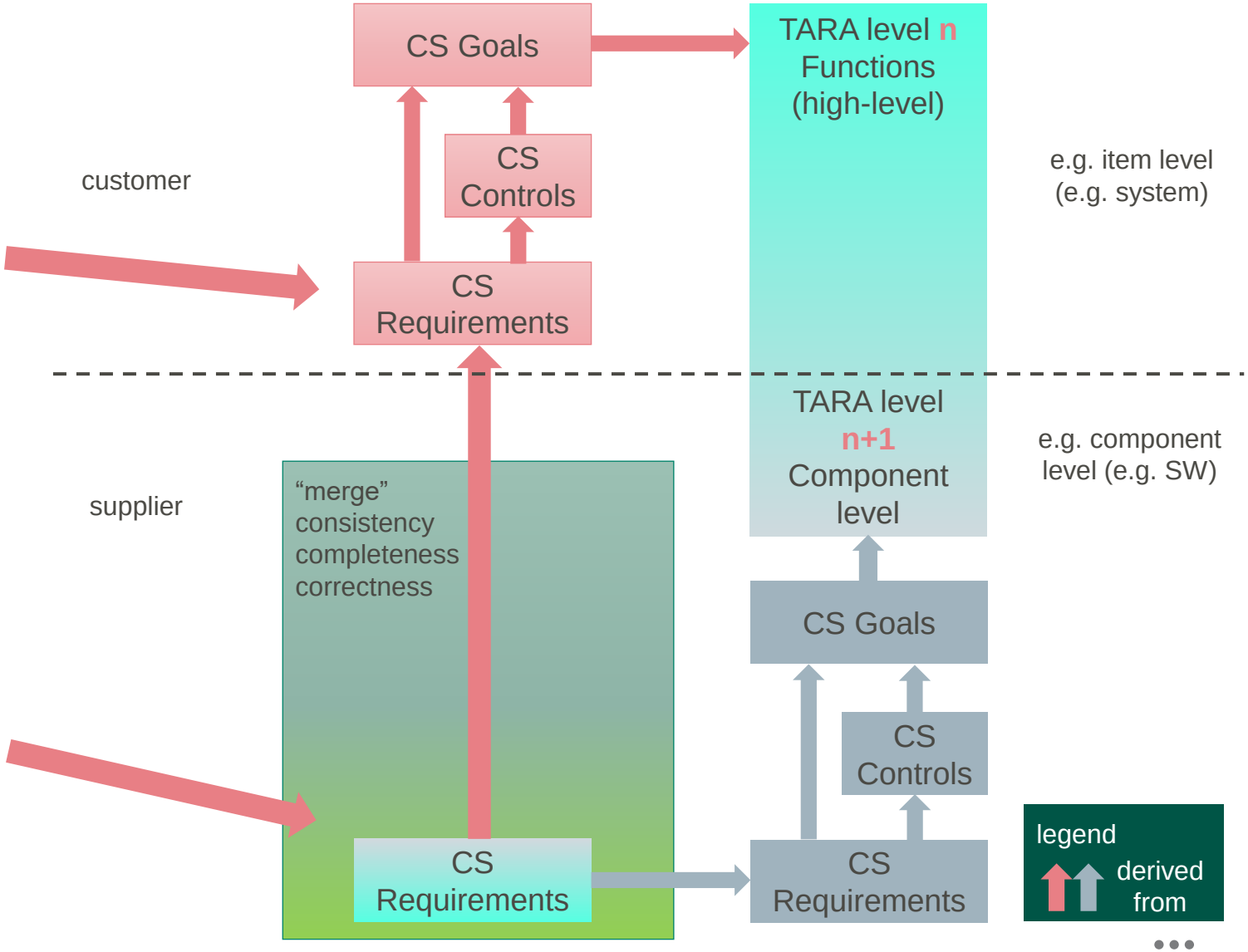
SynSpace Group GmbH & I.S.C.N. | Thomas Liedtke; Richard Messnarz | © 2025 | version 1v1

Vertraulichkeitsstufe: internal

Objectives for the Implementation of a TARA at Supplier Level

Experiences from Cybersecurity Assessments

- Confirmation/ proof of cybersecurity requirements received from a higher level from the customer (e.g. identification of the use of an HSM)
- Identification of new cybersecurity controls and requirements at the supplier's detailed level (e.g. based on assets that are not yet visible at a higher level)



SynSpace Group GmbH & I.S.C.N. | Thomas Liedtke; Richard Messnarz | © 2025 | version 1v1

Vertraulichkeitsstufe: internal

Typical Situation in Practice on Supplier Level (1)

Experiences from Cybersecurity Assessments

- Supplier carries out its TARA (in order to gain lead time) in parallel with the implementation of the customer's cybersecurity requirements.
  - Example: a software manufacturer starts with the processes SWE.1/SEC.2 (basis of cybersecurity requirements received from the customer) and MAN.7 (implementation of the TARA to derive additional cybersecurity requirements) in parallel.
- Cybersecurity requirements received from the customer/controls to be implemented can be taken into account in the supplier TARA or the necessity can be confirmed.
  - Example: rationale for the introduction of an HSM or SecOC
- Customer's cybersecurity requirements must be taken into account when verifying the cybersecurity goals/controls and requirements:
  - Consistency: in particular, external consistency with cybersecurity requirements already received must be ensured
  - Completeness: the cybersecurity requirements derived in the supplier TARA must complete the customer's cybersecurity requirements

Vertraulichkeitsstufe: internal

Typical Situation in Practice on Supplier Level (2)

Experiences from Cybersecurity Assessments

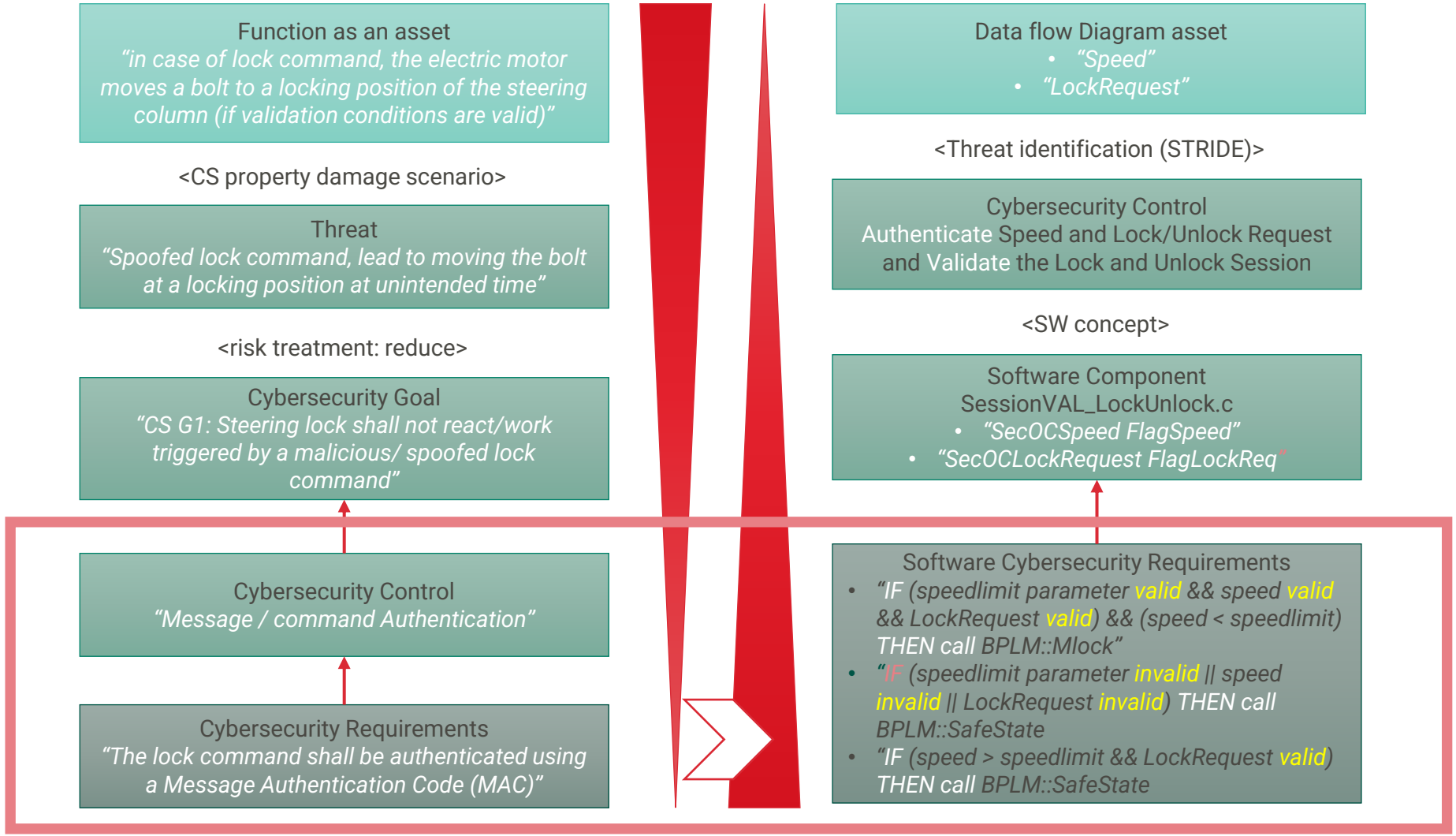
- Combination and merging of TARAs at different levels (if required)
- Specified cyber security goals at the supplier level have to be validated at the supplier level
- All existing requirements/components (in architectural design) must ultimately be traceable to a corresponding (valid) source.
  - Analysis results (result of a TARA) are possible sources to which requirements/ components can be linked.

- To verify “merge” of the different sets of cybersecurity requirements following objectives (s. [ISO/SAE 21434:2021-9.5.2] (concept) as a base) have to be achieved generally:
  - completeness, correctness, and consistency with respect to cybersecurity goals
  - consistency with respect to cybersecurity claims

Vertraulichkeitsstufe: internal

Relationship of CS System and CS Software requirements – verification | validation

Experiences from Cybersecurity Assessments



Vertraulichkeitsstufe: internal

Agenda

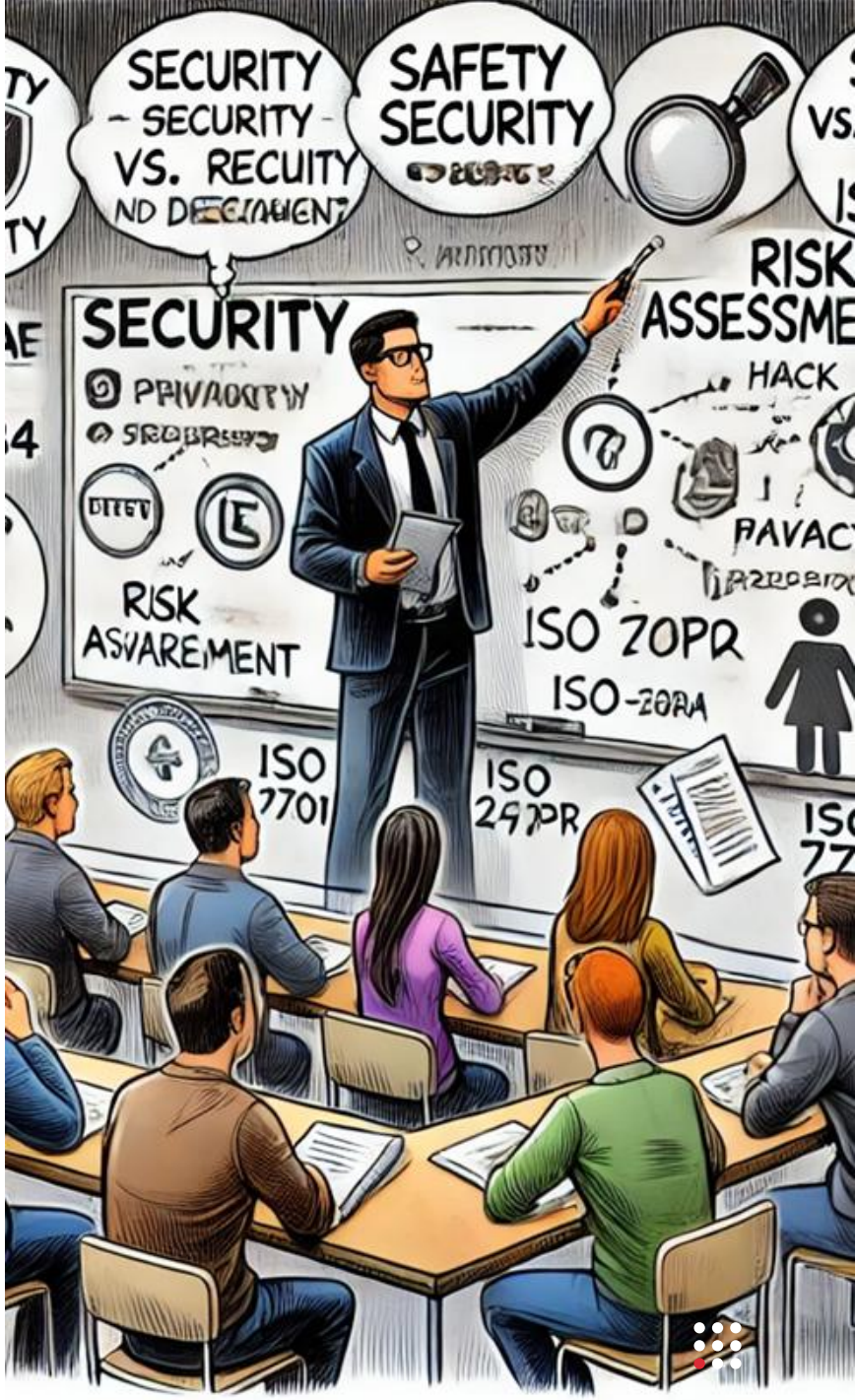
Experiences from Cybersecurity Assessments

- Motivation
- Automotive SPICE® for Cybersecurity PAM 2.0
- Experiences from Cybersecurity Assessments
- Summary
- Bibliography

Vertraulichkeitsstufe: internal

Lessons Learned
Summary

- Automotive SPICE© for Cybersecurity
  - Still not 100% compliant with ISO/SAE 21434
    - With PAM 2.0 now better alignment achieved
  - Includes more than just the road user as stakeholder
  - Focuses on risk reduction
  - Does not cover requirements outside the direct project environment (CSMS/ ISO PAS 5112)
  - Risk management (MAN.7) process is the decisive



Vertraulichkeitsstufe: internal

Agenda

Experiences from Cybersecurity Assessments

- Motivation
- Automotive SPICE® for Cybersecurity PAM 2.0
- Experiences from Cybersecurity Assessments
- Summary
- Bibliography

Vertraulichkeitsstufe: internal

Bibliography

- See further articles, presentations, and publication from Prof. Richard Messnarz and Thomas Liedtke PhD

AUTOMOTIVE SYS®

EURO SPI² 2024
European System, Software & Service Process Improvement & Innovation
In cooperation with initiatives in Asia, Africa and USA