News on the Automotive SPICE® for Cybersecurity 2.0 Update

INTACS Central and Eastern European Regional Event

Dr. Thomas Liedtke

Dr. Richard Messnarz

INTACS®

Agenda

News on the Automotive SPICE® for Cybersecurity 2.0 Update

1 | Introduction

2 | Instances in Practice

3 | Training Content Update in Relation to SEC.1-SEC.4

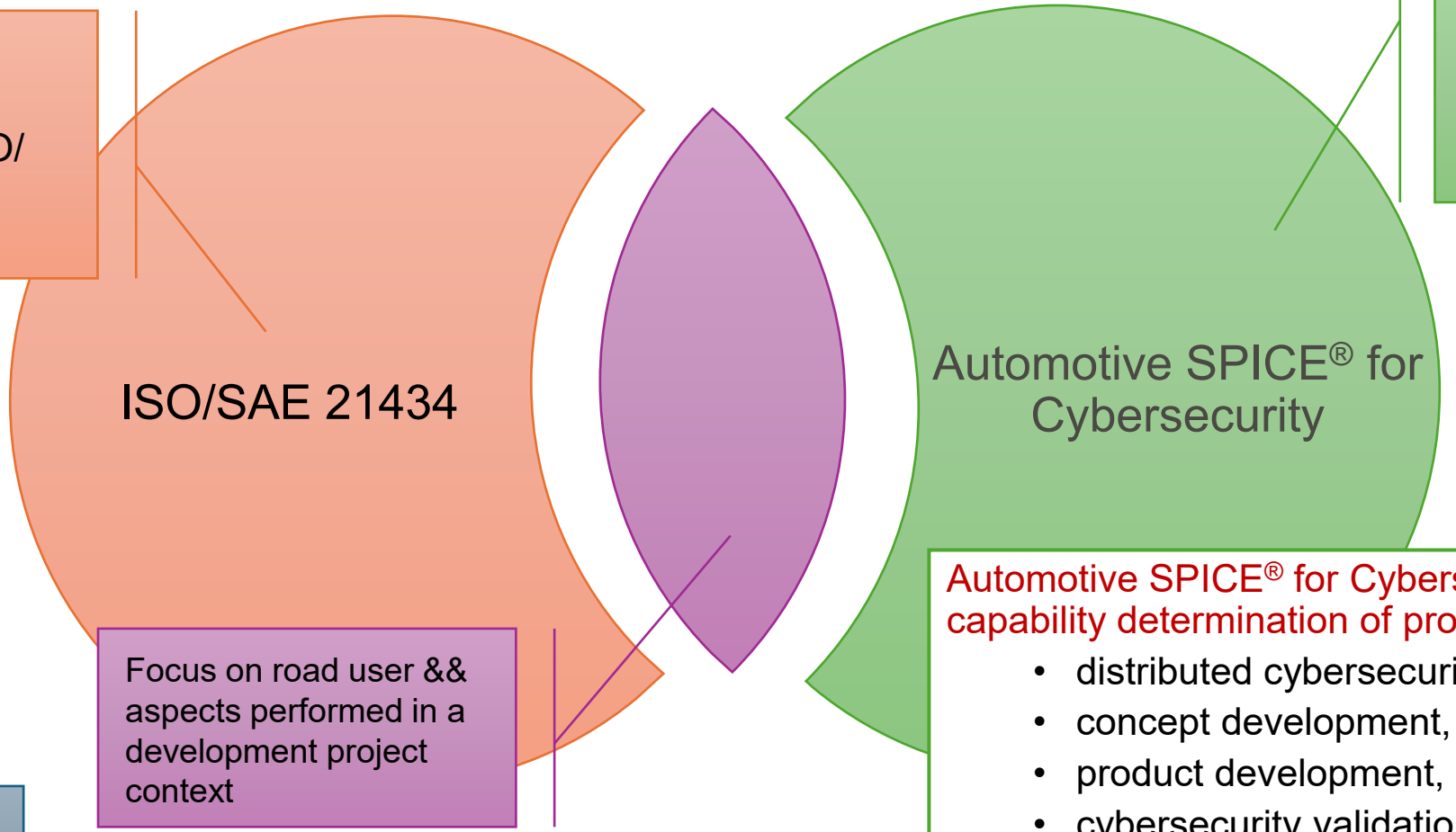
4 | Outlook into Further Changes Due to SDV and AIDVs

INTACS®

The scope and content are still slightly different

1 | Introduction

≠ Development project context: addressed by ISO/ PAS 5112 topics (audit)



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

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

Size of bubbles are not representing the number of requirements

Automotive SPICE® for Cybersecurity supports capability determination of processes for

- distributed cybersecurity activities,
- concept development,
- product development,
- cybersecurity validation, and
- threat analysis and risk assessment

Terminology used

1 | Introduction

- Alignment of terms (e.g., regarding Automotive SPICE® PAM 4.0)
  - Process Capability ~~Assessment~~ → Determination
  - Organizational ~~Lifecycle~~ Processes category
  - Security Process Group → Cybersecurity Process Group
  - ~~Missing~~ evidence ~~ACSMS and ASPICE~~ → Evidence of corrective actions // ACSMS withdrawn standard //
  - Rating ~~consistency~~ → Rating rules
  - Work Product → Information Item
  - …

Terminology aligned with Automotive SPICE® PAM 4.0 and fewer discrepancies compared to ISO/SAE 21434

Legend:
- ~~Strike through~~: skipped in version 2.0
- Orange: new in version 2.0

Relationship to ISO/SAE 21434

1 | Introduction

- [..] 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
- 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

*) Automotive SPICE® for Cybersecurity PAM 2.0

Legend:
- ~~Strike through~~: skipped in version 2.0
- Orange: new in version 2.0

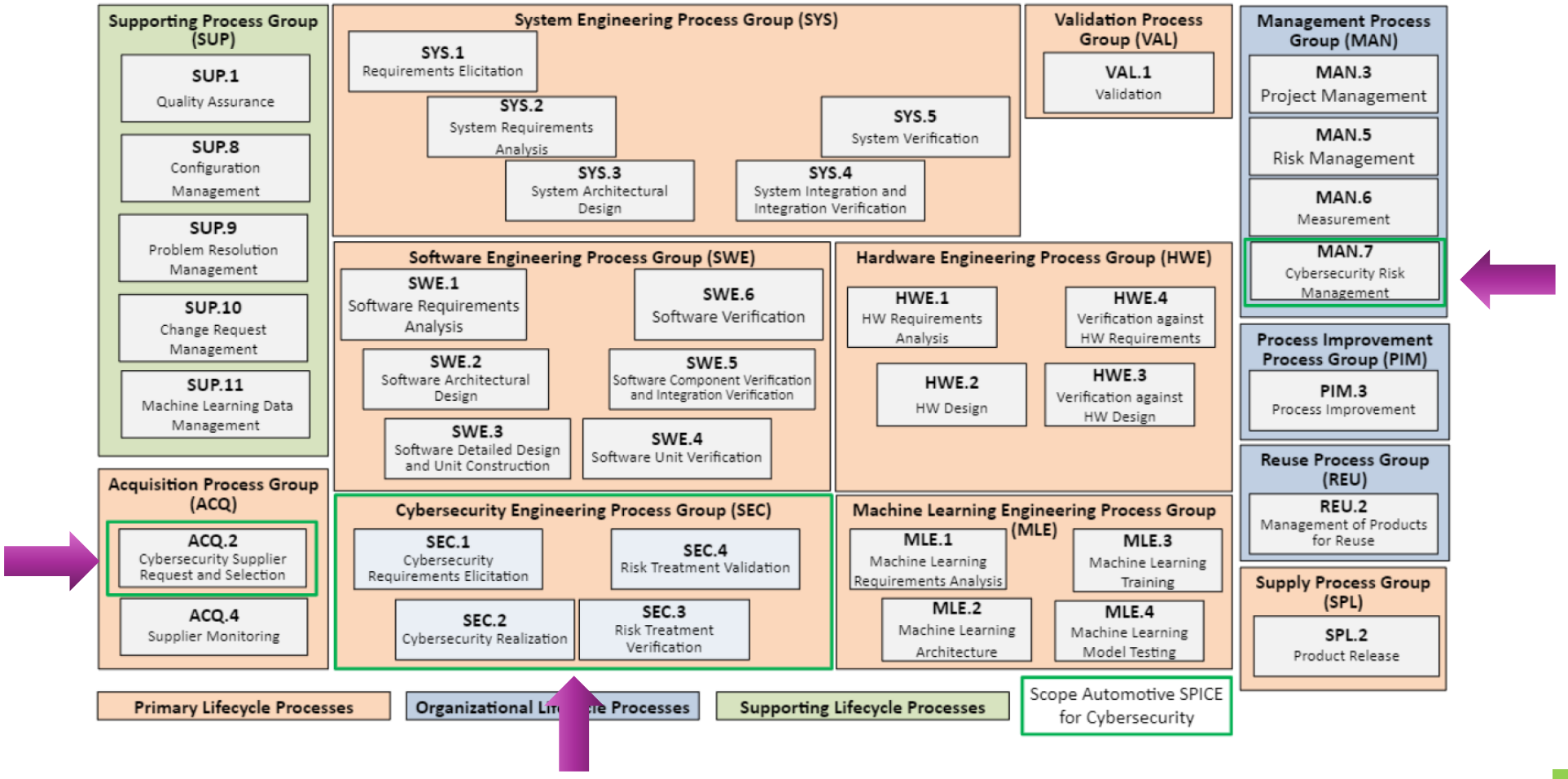
Rationale for Assessment Scope

1 | Introduction

- Risk Treatment Validation
  - process is focused on the cybersecurity goals where the validation process refers to all stakeholder goals or stakeholder requirements.
  - 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
- SEC.4 purpose declares that it is to confirm that the integrated system achieves the associated cybersecurity goals.
- VAL.1 purpose is to provide evidence that the delivered product satisfies the intended use expectations in its operational target environment.
- If the purposes of the respective processes are compared this becomes apparent.
- 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.
- 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.

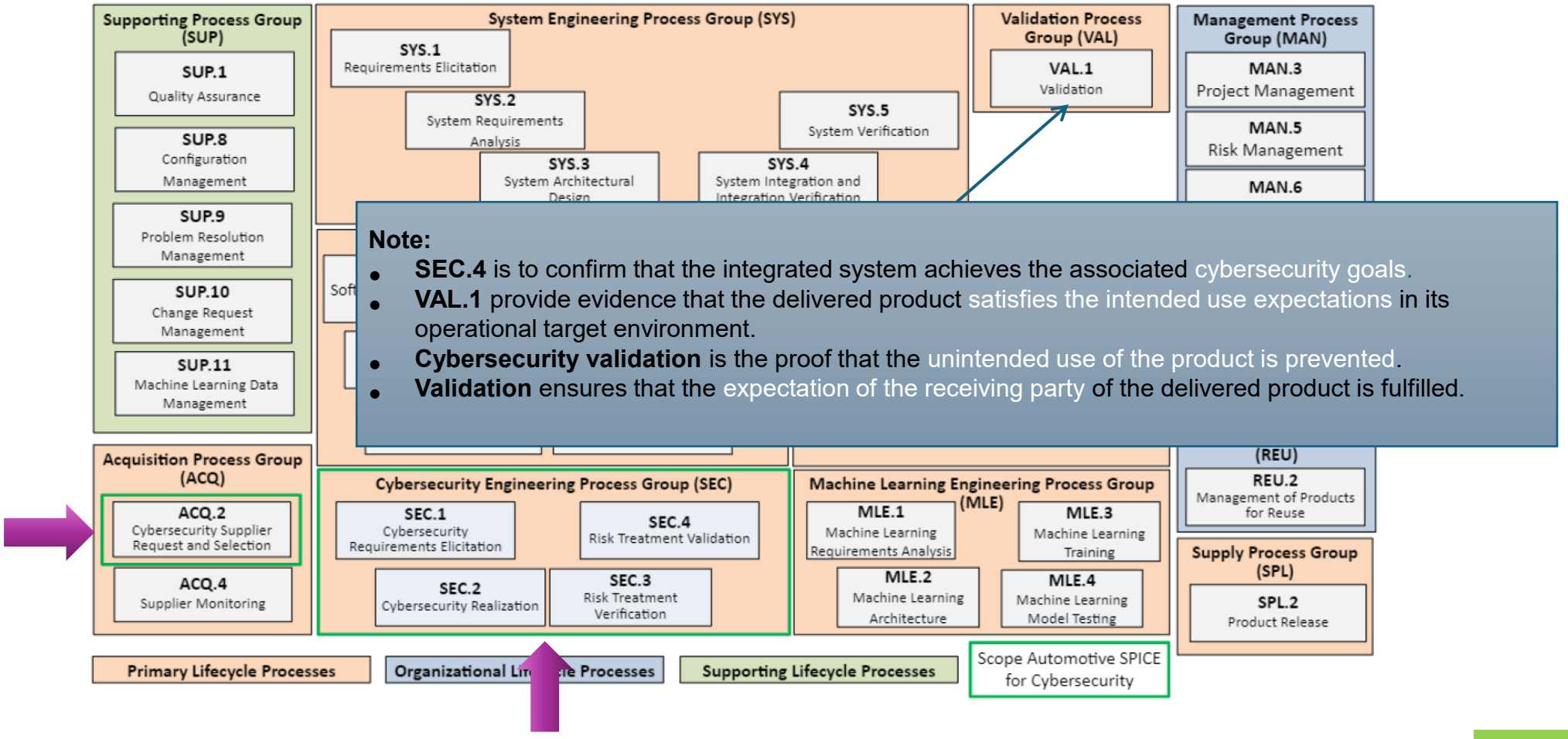
VDA – QMC | Automotive SPICE® | Process landscape

1 | Introduction



VDA – QMC | Automotive SPICE® | Process landscape

1 | Introduction



Agenda

News on the Automotive SPICE® for Cybersecurity 2.0 Update

1 | Introduction

2 | Instances in Practice

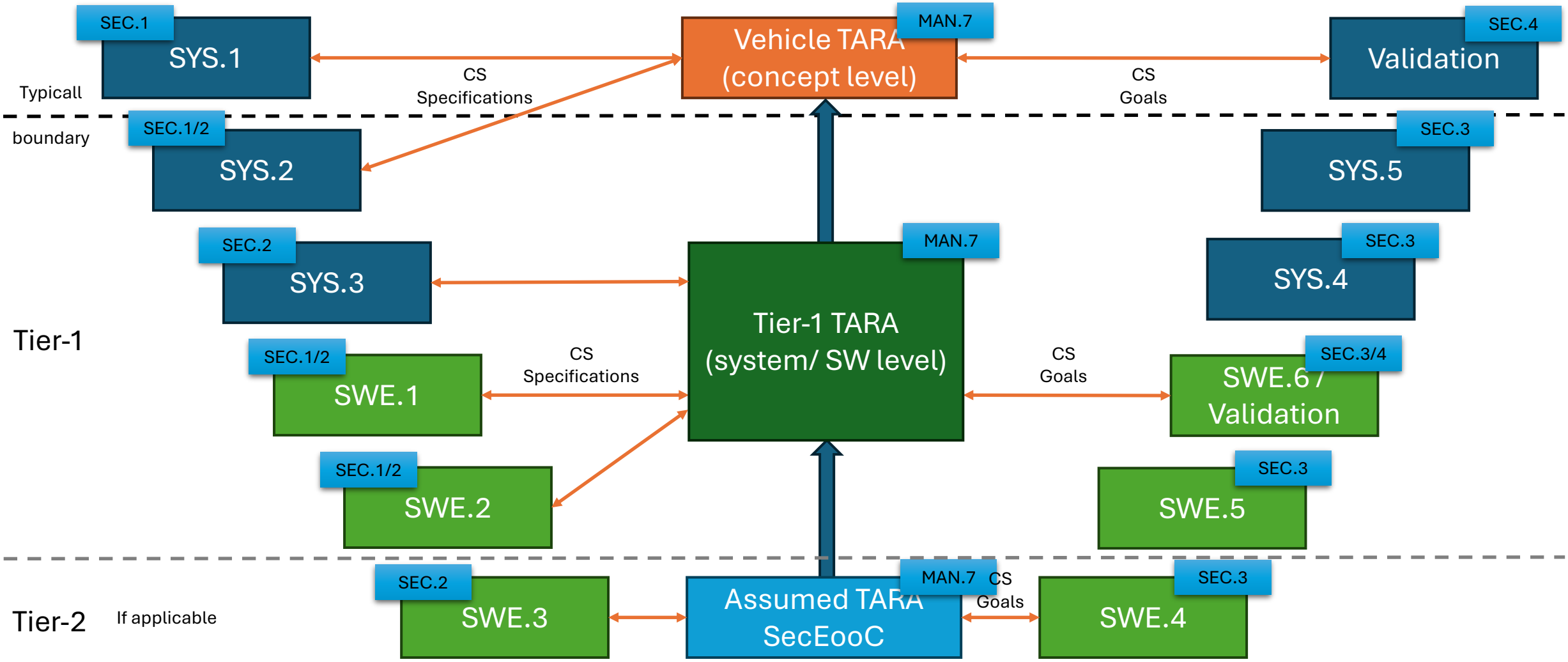
3 | Training Content Update in Relation to SEC.1-SEC.4

4 | Outlook into Further Changes Due to SDV and AIDVs

INTACS®

Assignment processes Automotive SPICE® PAM 4.0 and Cybersecurity PAM 2.0

2 | Instances in Practice



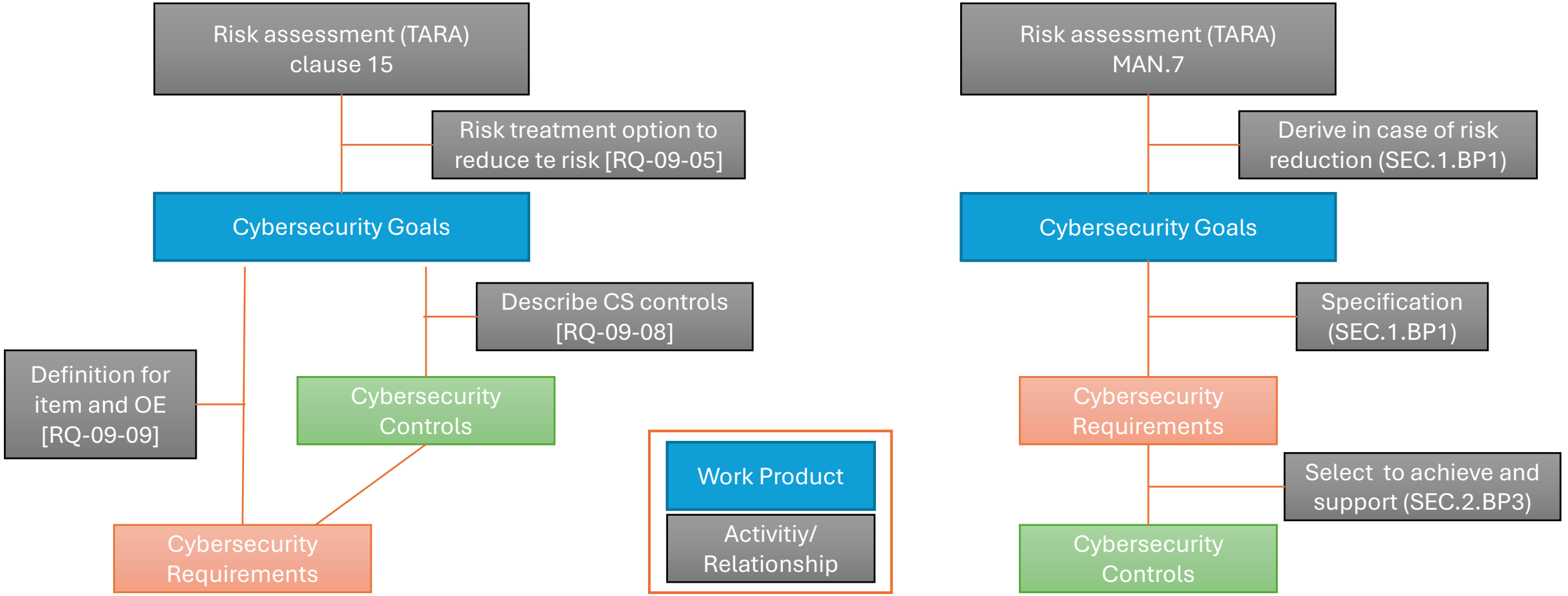
SEC.1 and SEC.2 topics

2 | Instances in Practice

- Experienced Automotive SPICE assessors know that the way things are done in projects often deviates from Automotive SPICE specifications (especially the order in which they are done).
- The reason for this is simply that Automotive SPICE® specifies what needs to be done but does not prescribe a strict order in which it must be done.
- Example: In Automotive SPICE, a requirements process comes first, followed by an architecture process. In practice, a project will never wait until the requirements are finalized before architecture work begins. There is always parallel development, where the requirements influence the architecture, and the architecture development can lead to new or changed requirements.
- It's the same here with Automotive SPICE for Cybersecurity: it looks like cybersecurity requirements come first and then implementation. During project lifetime updates of TARA can become necessary (e.g., new knowledge about vulnerabilities) which can motivate further requirements.
- The point is that CS requirements cannot be derived immediately from CS goals. Rather, the architecture must be analyzed, CS controls must be mapped to architectural elements, and CS requirements must be derived from CS controls (see next slide).

Differences between ISO/SAE 21434 and Automotive SPICE® for Cybersecurity

2 | Instances in Practice



3.1.14 CS Control: measure that is modifying risk

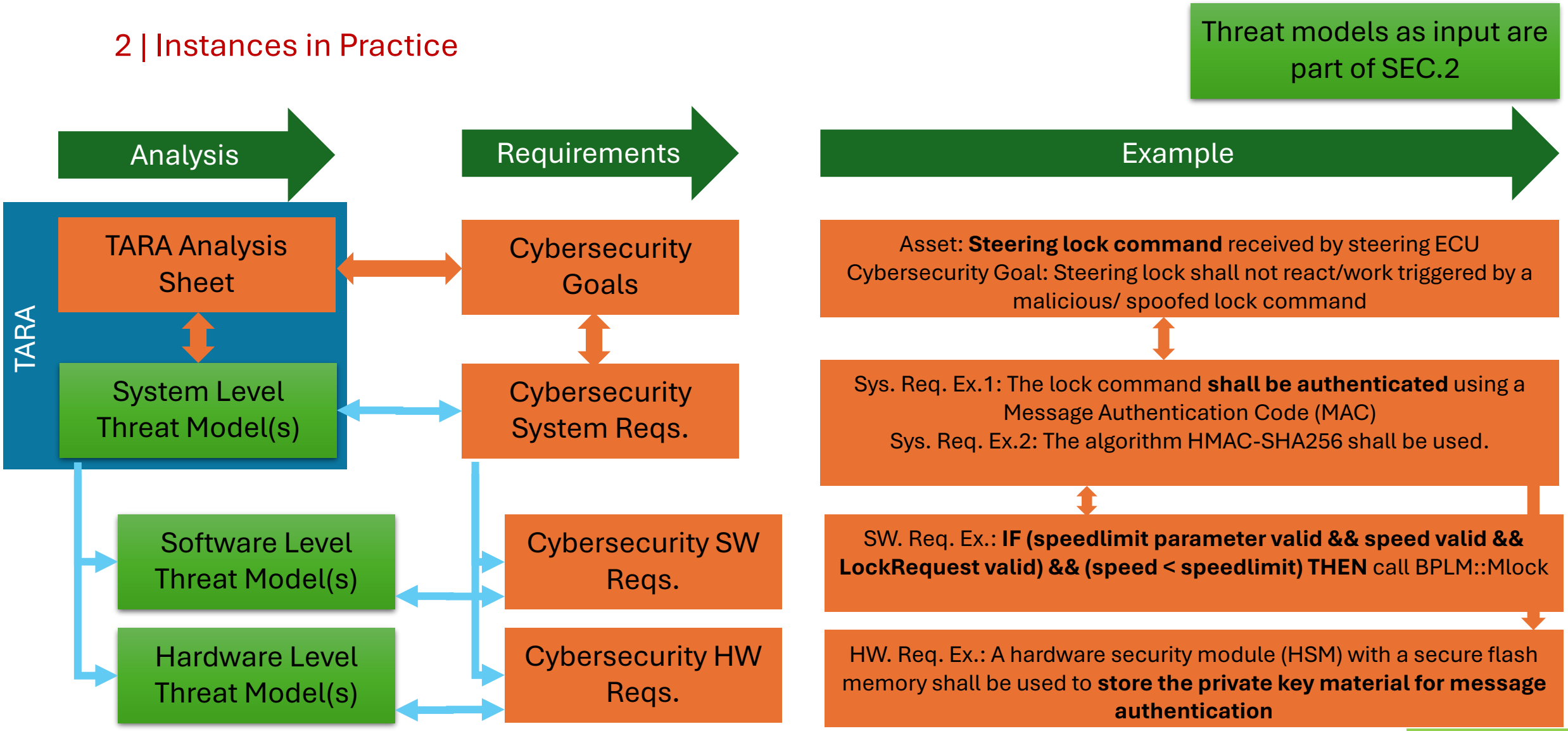
3.1.16 CS Goal: concept-level CS requirement associated with one or more threat scenarios

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

SEC.1 Cybersecurity Requirements at Different Levels

2 | Instances in Practice



Traceability and Consistency - Overview of bidirectional traceability and consistency

2 | Instances in Practice

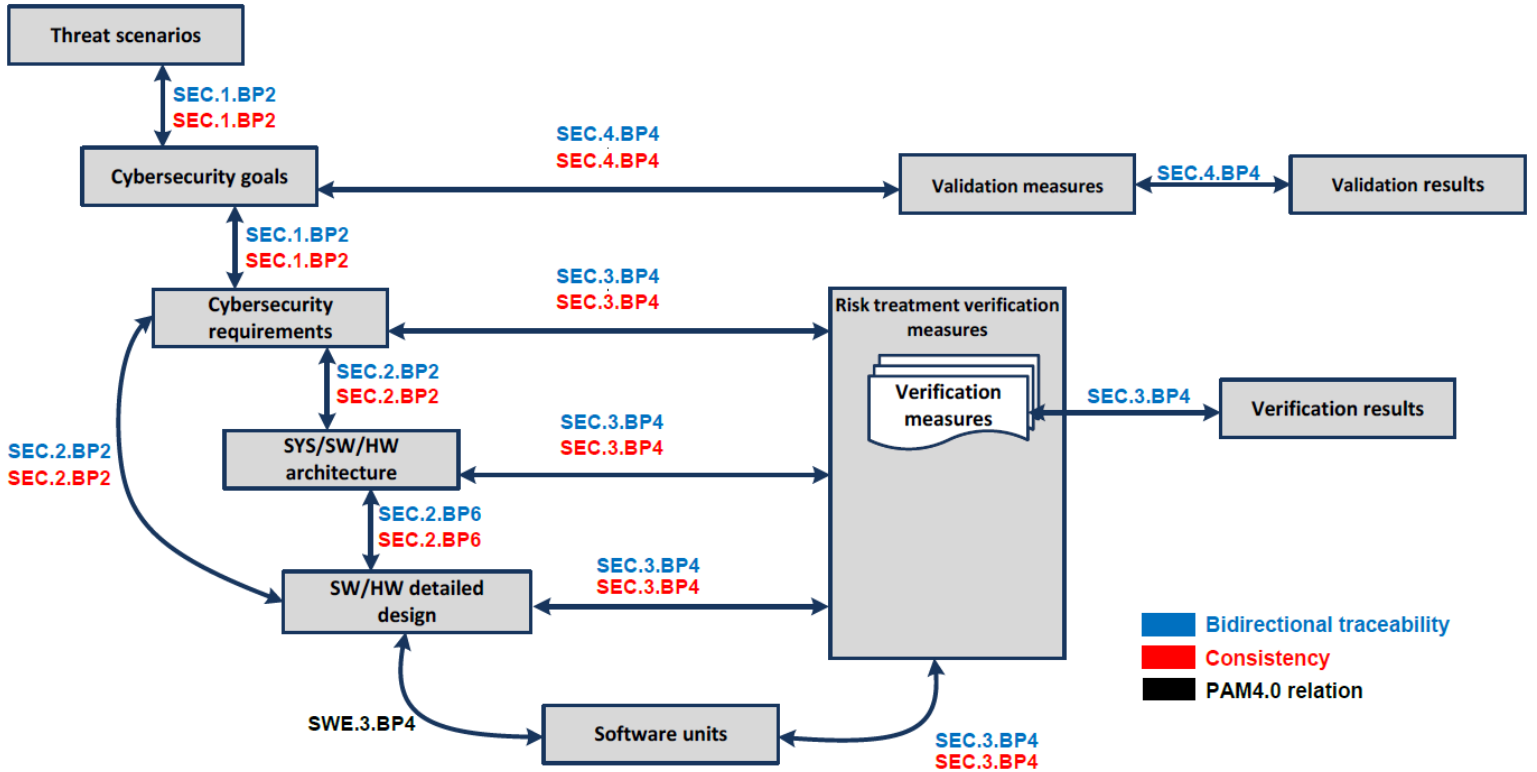


Figure 7 — Bidirectional Traceability and Consistency

Agenda

News on the Automotive SPICE® for Cybersecurity 2.0 Update

1 | Introduction

2 | Instances in Practice

3 | Training Content Update in Relation to SEC.1-SEC.4

4 | Outlook into Further Changes Due to SDV and AIDVs

INTACS®

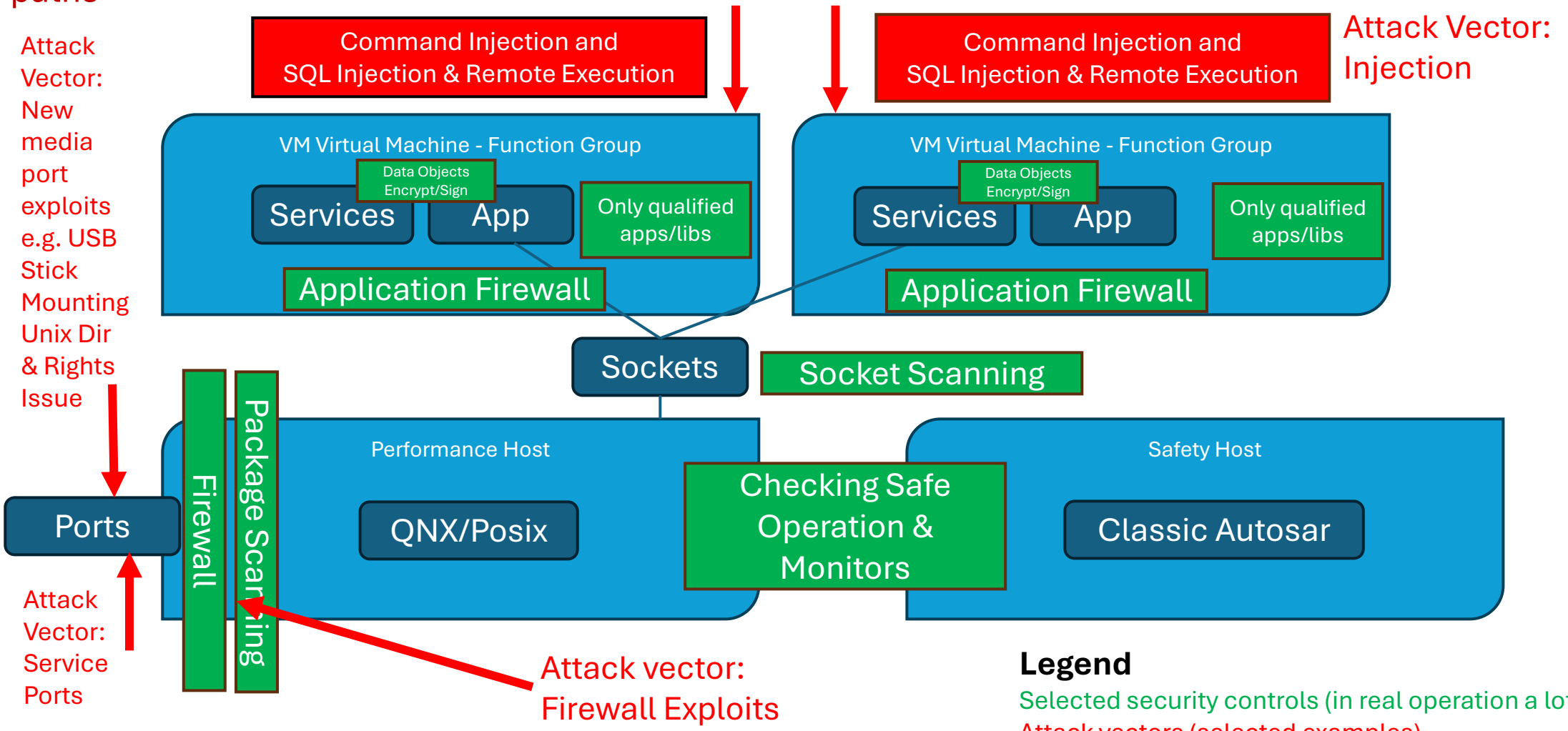
Training Content Update in Relation to SEC.1-SEC.4

The ASPICE for CS working group integrates best pratices from the field into the training to explain the BPs and background

New results from CYBERTESTER EU Project / SOQRATES

Major Change: Beside the ECU and Classic Autosar based CS architectures, the training addresses server and SDV architectures of vehicles as well

Future SOA based architectures will grow in size dynamically, creating a fast set of potential attack paths



Legend

Selected security controls (in real operation a lot more)

Attack vectors (selected examples)

Example successful attacks reported on servers

While the old training material focused on ECUs, the new one has ECU and Server included

- Run shell scripts or install unauthorized software via USB
- Direct Memory Access attack against USB 3.x
- Specially prepared media files can be used to tamper media engine services, Bluetooth, and Wi-Fi stacks
- Adding extra code to a digital music file, researchers were able to turn a song burned to CD into a Trojan horse
- Apps that are directly installed by the Driver into the MM System or his mobile connecting to the car
- Vulnerability of the OnBoard browser of the car
  - intercepting the encrypted connection between car connectivity app and Server
  - Remote code execution by exploiting the vulnerable internet service on Linux QNX MMX Service
  - Default user account password found in GPS tracker apps
- Malicious apps often disguise themselves as tools designed to enhance a car's in-vehicle infotainment (IVI) system or improve performance. But instead of providing genuine benefits, they can steal personally identifiable information (PII), commit fraud, deploy ransomware, or serve adware.

Agenda

News on the Automotive SPICE® for Cybersecurity 2.0 Update

1 | Introduction

2 | Instances in Practice

3 | Training Content Update in Relation to SEC.1-SEC.4

4 | Outlook into Further Changes Due to SDV and AIDVs

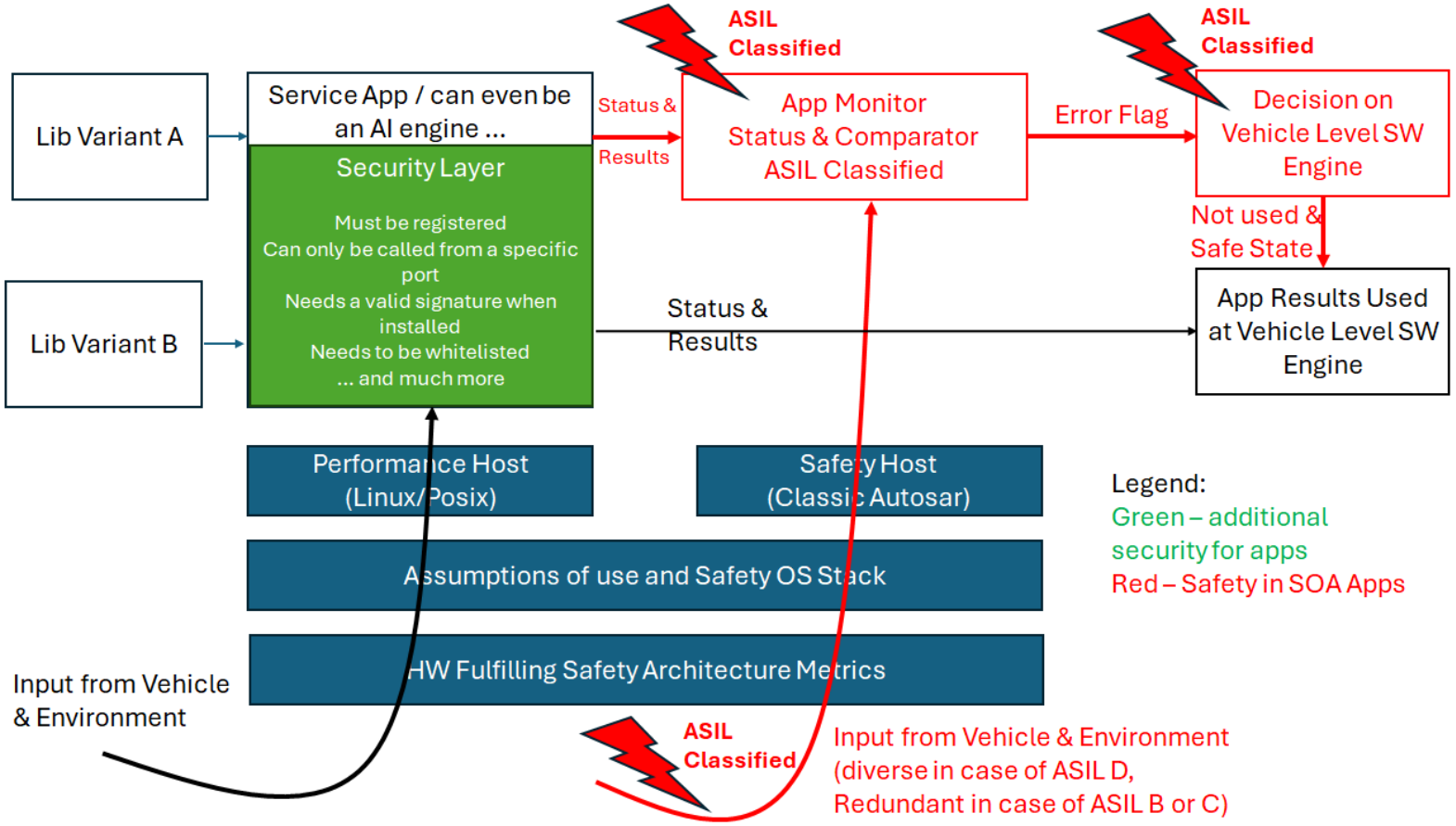
INTACS®

Outlook into Further Changes Due to SDV and AIDVs

The competition between Europe and China leads to a demand of Software Defined Vehicles and AI Defined Vehicles where SW apps and SOAs Service Oriented Architecture Competition will become the decisive factor to win.

SOA Architectures of SDVs and AIDVs lead to new challenges

In an SOA and App based framework the cybersecurity and safety design patterns will adapt and this will impact the next versions of cybersecurity materials and understanding

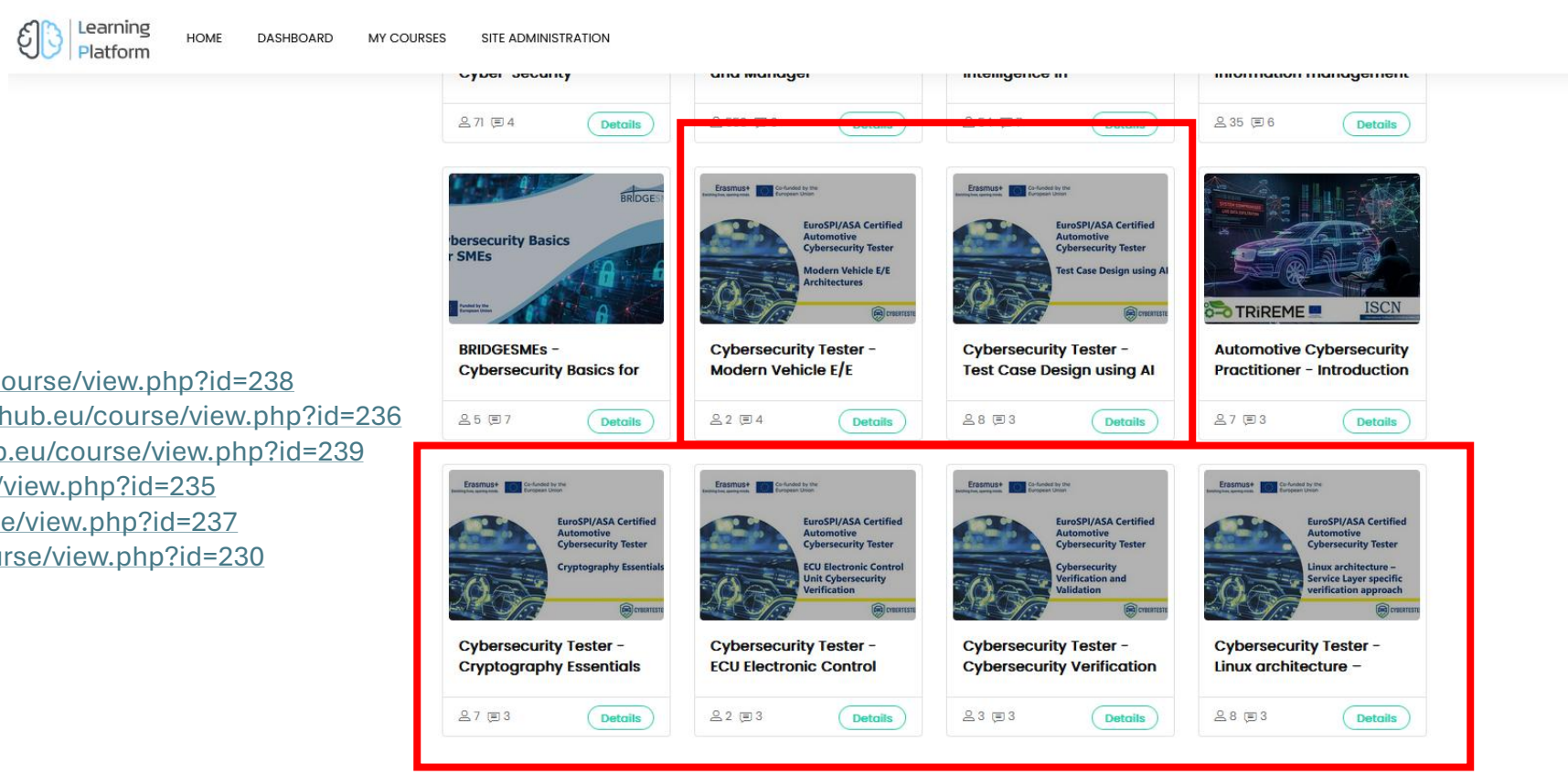


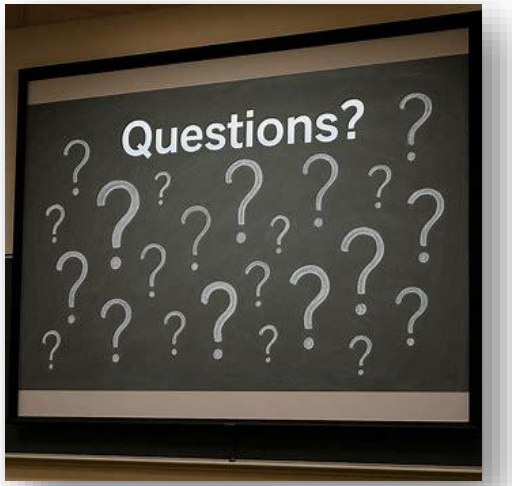
Free MOOCS from Cybertester

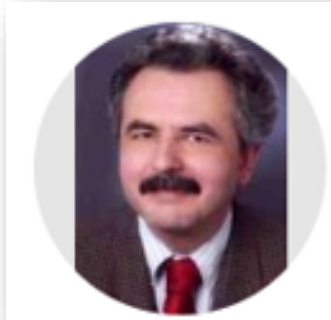
- Integrated to the Skills Hub of the Automotive Skills Alliance
- https://learn.skills-hub.eu/

Register for free
Receive a Link by Email
Confirm and login

Vehicle Servers : https://learn.skills-hub.eu/course/view.php?id=238
Test Case Design with AI: https://learn.skills-hub.eu/course/view.php?id=236
Modern Vehicle Arch.: https://learn.skills-hub.eu/course/view.php?id=239
ECU level: https://learn.skills-hub.eu/course/view.php?id=235
Verification: https://learn.skills-hub.eu/course/view.php?id=237
Cryptography: https://learn.skills-hub.eu/course/view.php?id=230







Dr. Thomas Liedtke

Consultant

Mobil: +49 173 676 40 93
E-Mail: thomas@tliedtke.onmicrosoft.com
LinkedIn: https://www.linkedin.com/in/thomas-liedtke/

Dr. Richard Messnarz

Director

I.S.C.N. GesmbH
Karl Morre Straße 86 A-8020 Graz, Austria
Tel.: +43 316 811198
E-Mail: rmess@iscn.com
Web: www.iscn.com