Lessons learned from a joint approach

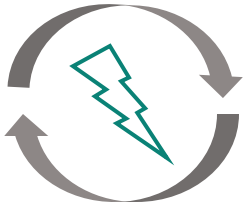
Automotive SPICE®, ISO 26262 and ISO 21434 assessment

Sandeep Chandrashekar (Infineon),
Janine Funke (UL), Bhaskar Vanamali (UL)
Alexander de Jong (UL)

Problem Statement

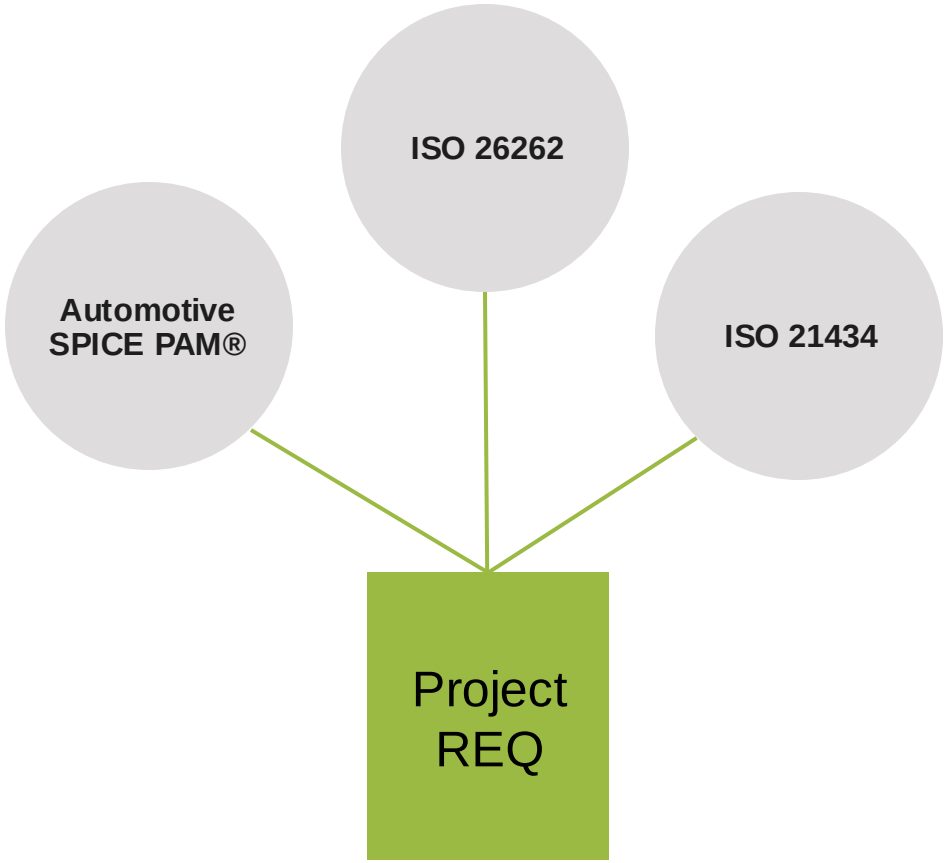
- Audits and assessments are needed to show compliance
- Synergies between standards can be used

compliance
capacity



time pressure
budget

- An organizational CSMS audit will not cover all the projects
- Bouquet of applicable standards requires different audits and assessments



Problem Statement
Standard evolution

Automotive SPICE ®

› V 2.5 → V 3.1 → V 4.0 ...

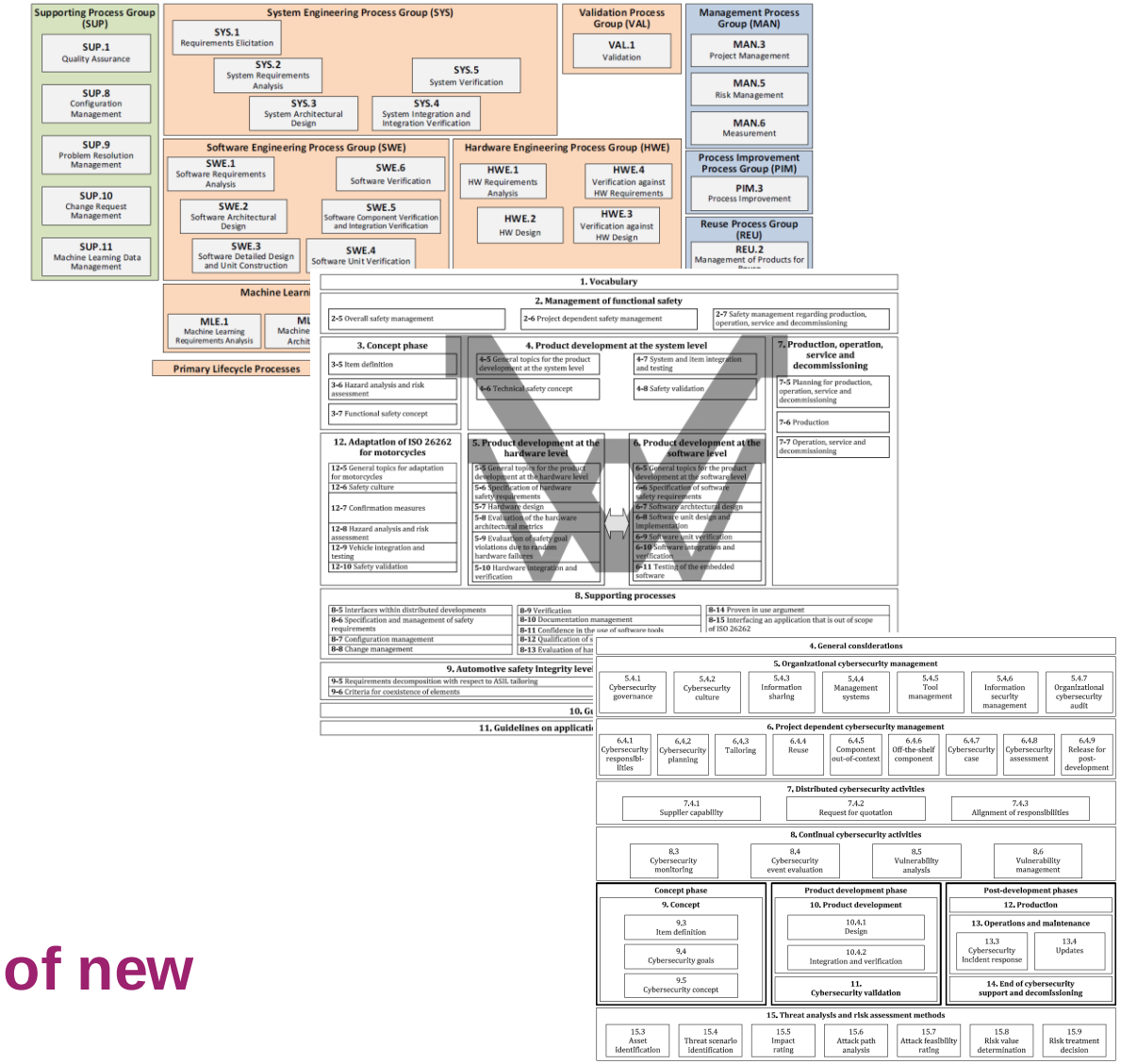
ISO 26262

› 1st edition - 2011 → 2nd edition – 2018 ...

ISO 21434

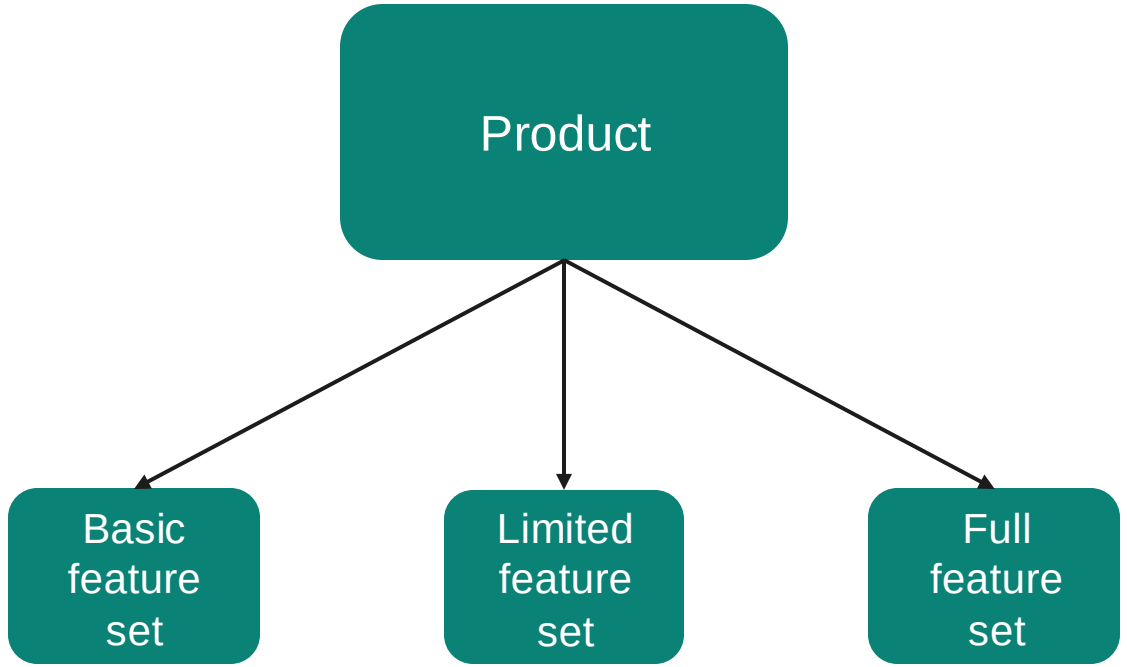
› 1st edition 2021 ...

› **Re-Assessments after publication of new standard version required**



Problem Statement
Product instances

- Typically, a product has
  - a basic feature set
  - a limited feature set
  - and a full feature set
- All sets have to be checked in terms of Functional Safety and Cybersecurity, arguably even against Automotive SPICE®
- **5** product variants planned
  - Each with at least two **(2)** customizations
- **5** times maintenance
- = 50 overall variations



50 variations * 3 standards = 150 audits/assessments

Standard comparison
Similarities and differences

Aspect	Automotive SPICE®	ISO 26262	ISO 21434
Processes	Yes	Yes	Yes
Quality mgmt system	Yes	Yes	Yes
Model	Detailed assessment model	Objectives and requirements	Objectives and requirements
Interpretation Guidance	Base practices and information items	Detailed guidance	Little to no guidance
After SoP	No recommendation	Complete life cycle	Complete life cycle
Assessment requirements	Process assessment model, VDA and intacs	Little guidance	Little guidance

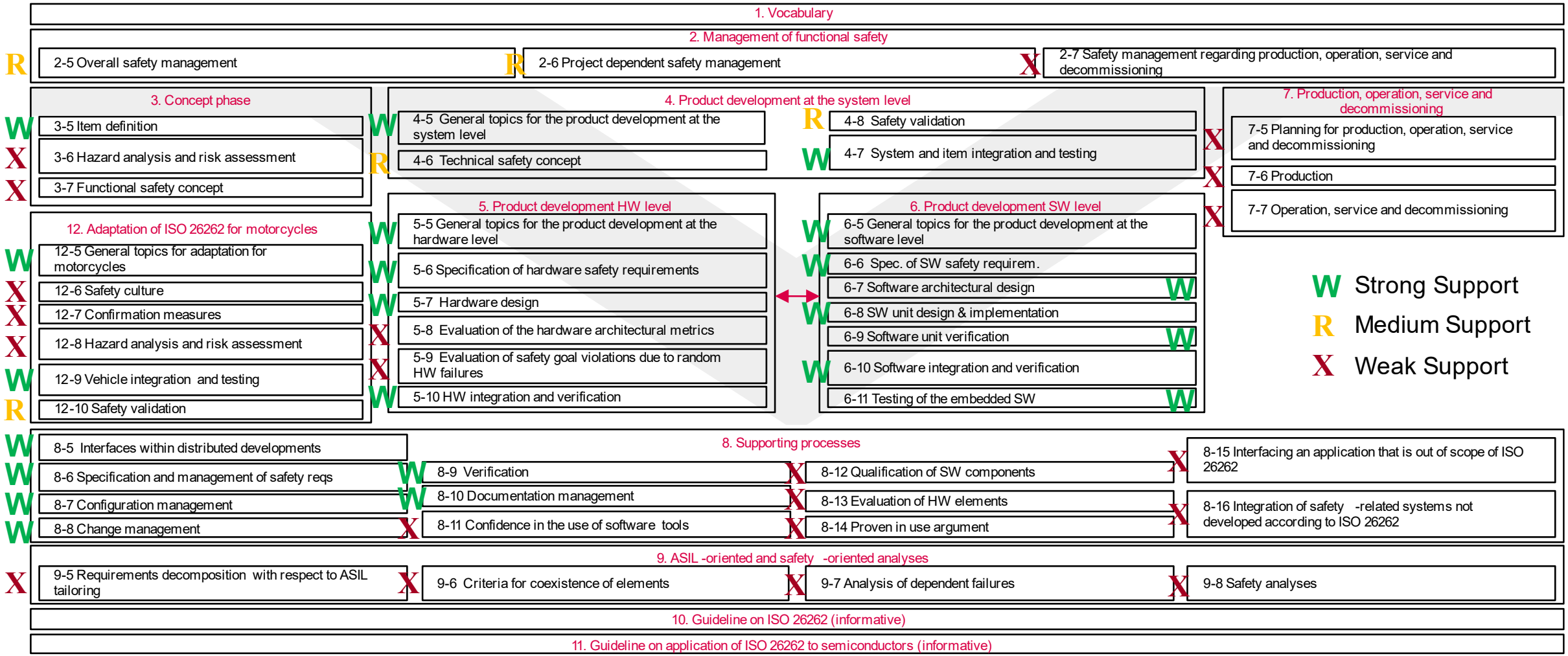
Difference between Audit and Assessment: FuSa, CS

- **Audit:** FuSa and CS primarily evaluate suitability of processes
- **Assessment:** FuSa and CS primarily evaluate technical WP content
- Implementation of processes should be evaluated in assessment and audit
- Process audit based on ISO/SAE 21434 or ISO 26262 :

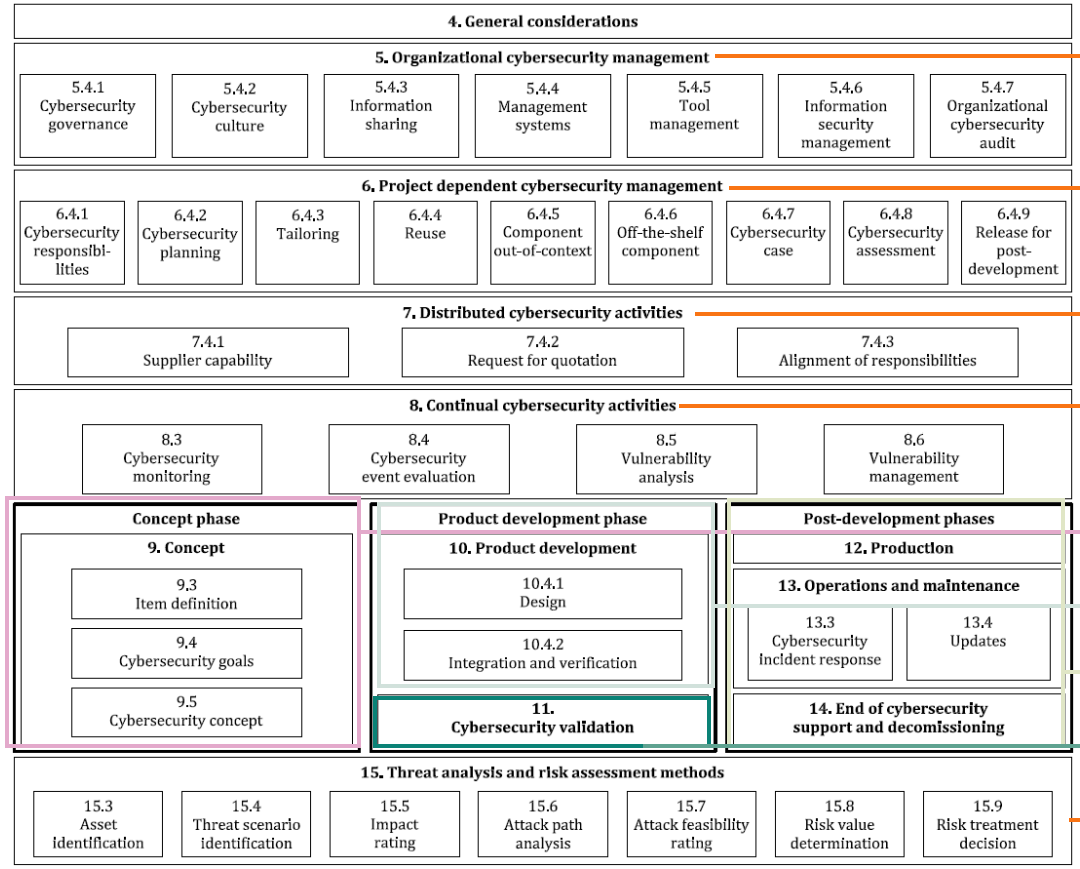
  No specific guidance on how to conduct an assessment within ISO SAE 21434 and ISO 26262, but..

  …results of the process audit as input for an assessment.

Automotive SPICE® 4.0 coverage of ISO 26262



Automotive SPICE® 4.0 coverage of ISO 21434



☑ MAN 3 with Capability level 3

☑ MAN 3

☒ ACQ extension

⊘ Weak support

☑ SYS & SWE

☒ SYS & SWE

⊘ Weak support for Post-development phases

☑ VAL

⊘ Weak support

Approaches for a combined evaluation (FuSa view)

1

– **Link the ISO 26262 requirements/objectives directly to an ASPICE® PAM**

› Huge effort to check all requirements/objectives

› Only one rating / reporting can be done, that is a combined answer for ISO 26262 and ASPICE®

› All requirements from ISO 26262 can be checked

2

– **Using the hybrid approach of ASPICE® with SS 7740**

› The current SS 7740 is not fully implemented as a hybrid approach

› The SS 7740 is an extensive list of BP's that is difficult to manage within an assessment

› It is not always clear if a BP of SS 7740 is already covered with a basis BP, and a note would be more appropriated

› Separate Report is difficult, because of the overlap to ASPICE® and SS 7740

3

– **Create a PAM that covers all ISO 26262 objectives and requirements, and evaluate both PAMs in parallel**

› The FuSa PAM can be used as well independent from ASPICE®.

› The PAM can be linked to ASPICE® and the overlap can be evaluated once.

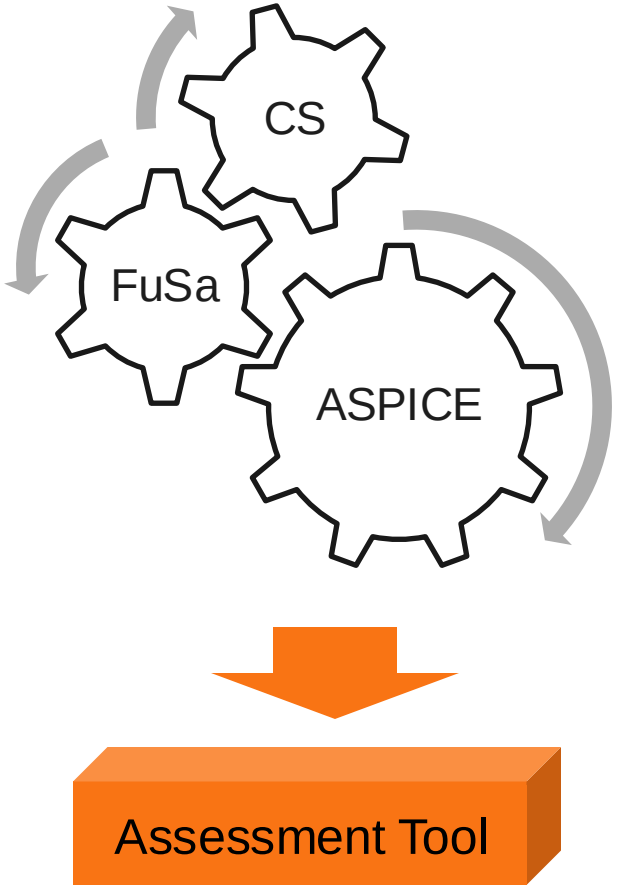
› The questionaire for FuSa PAM was already used successfully.

› Separate reports can easily be created.

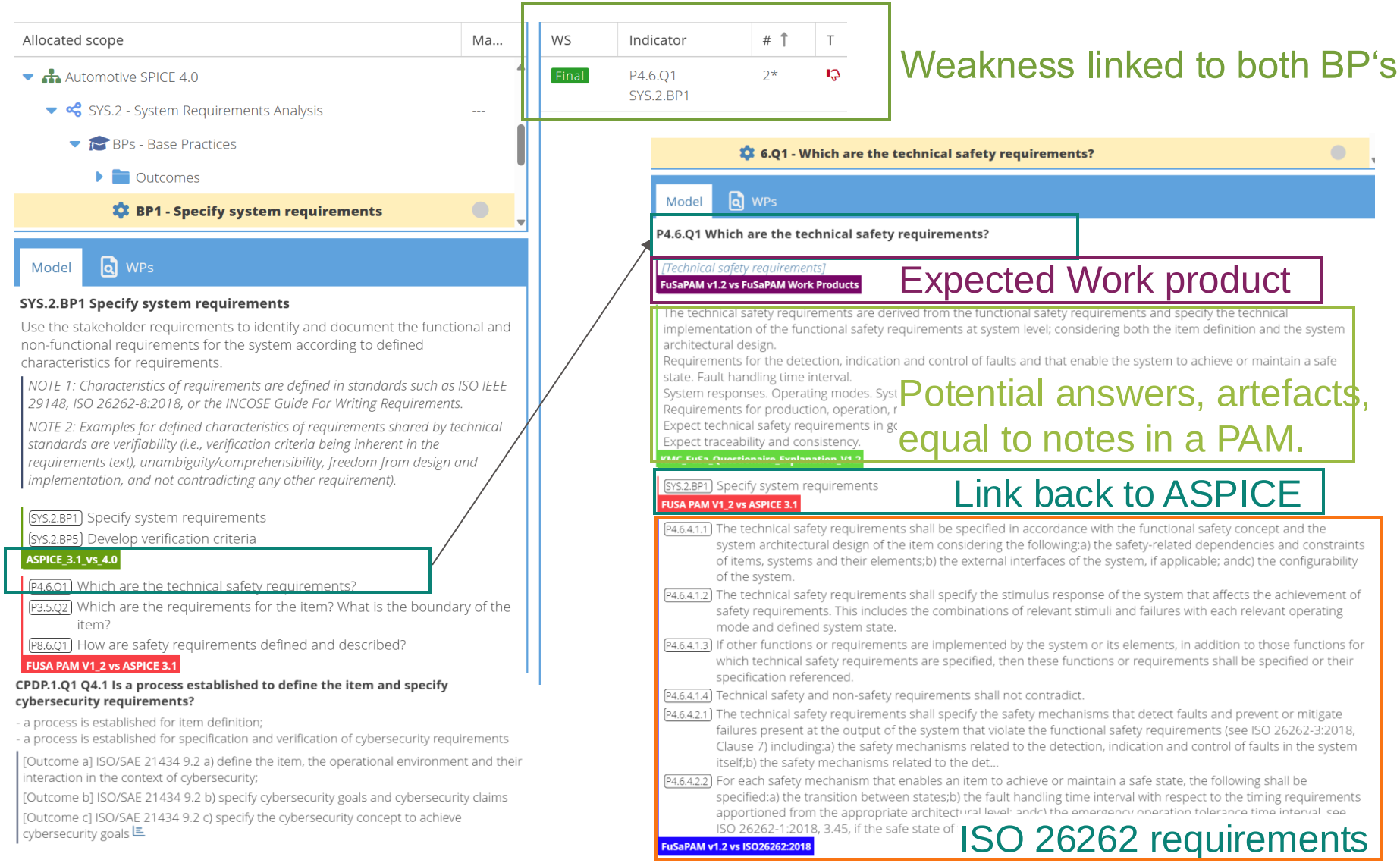
› Proprietary solution.

Our approach supported by the assessment tool

- Implementation using an assessment tool
- Approach 3 used for FuSa and similar for CS
- ISO PAS 5112 (& ISO 21434) was transformed into a model
- Implementation of cross references between all PAM’s
- Findings can be documented for all PAM’s within one step



Approach shown based on the assessment tool



Same approach used for CS:

- ISO PAS 5112 questions and guidance mapped to ASPICE ® processes (if possible) or creation of additonal categories
- Content from ISO 21434 as support

Configuration Management

- **Automotive SPICE®** provides the strongest requirements regarding configuration management:
  - 8 base practices
  - 8 output information item

- **ISO 26262:**
  - Builds upon an existing configuration management system
  - No detailed requirements regarding configuration management

- **ISO 21434:**
  - Builds upon an existing configuration management system
  - No detailed requirements regarding configuration management

Summary:

- Check against Automotive SPICE® covers all standards
- Specific check on artifacts of Functional Safety and Cybersecurity
- Appropriate implementation of access management
- How is configuration management established after SoP

- 5 global requirements stated
- 1 Work Product expected

5.4.4 Management systems

[RQ-05-11] The organization shall institute and maintain a quality management system in accordance with International Standards, or equivalent, to support cybersecurity engineering, addressing:

EXAMPLE 1 IATF 16949 [7] in conjunction with ISO 9001 [8].

c) configuration management; and

[RQ-06-11] The cybersecurity plan shall be subject to configuration management and documentation management, in accordance with 5.4.4.

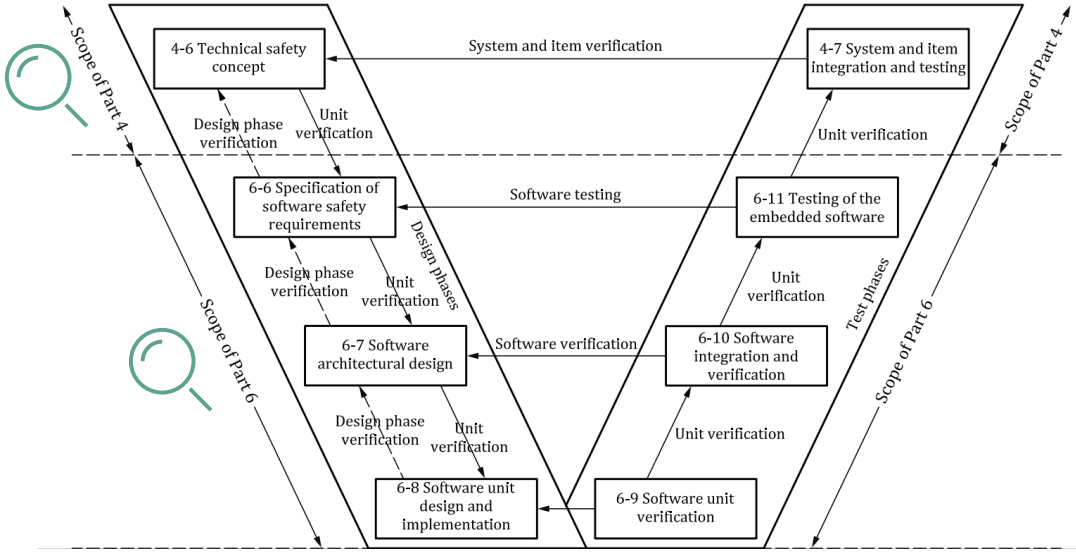
[RQ-06-12] The work products identified in the cybersecurity plan shall be subject to configuration management, change management, requirements management, and documentation management, in accordance with 5.4.4.

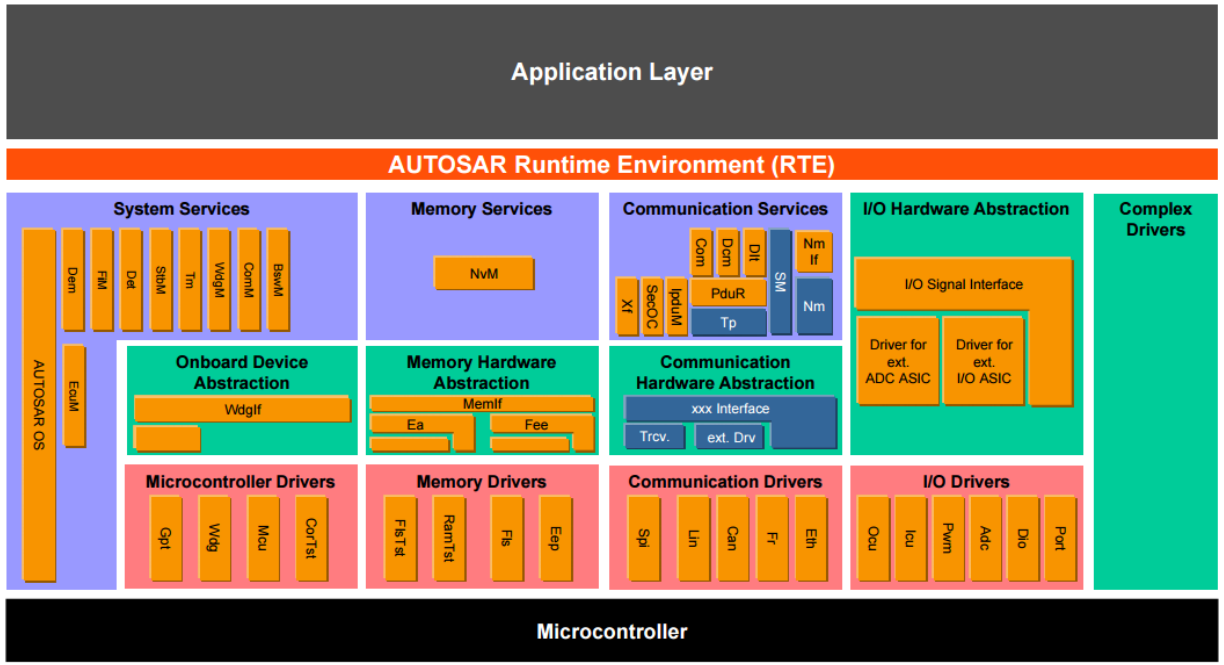
Software Architecture

- **Automotive SPICE®:**
  - 5 Base Practices
  - 4 Output Information Items
- **ISO26262:**
  - ASIL dependent requirements for Safety Analysis, Dependent Failure Analysis, Configurable SW, Annex D, Annex E, Qualification of SW components
  - 14 requirements
  - 4 work products
- **ISO 21434:**
  - Combines Requirement, Architecture, Design and Implementation
  - 7 requirements
  - 1 recommendation
  - 5 Work Products
- **Similarities:**
  - Static View
  - Dynamic View
  - Bi-direction Traceability

Software Architecture – Summary

- ASPICE® can be starting point but ISO 26262, ISO 21434 provide additional topics e.g. Analysis, methods on top of ASPICE® that need to be considered





- The system level input from Technical safety concept, Cybersecurity concept need to be considered in the SW architecture

Summary & Outlook

- Synergies are key as there is a pressure to have a shorter development time for developing a vehicle and its components, it can save time if done precisely
- For safety such questions need to be developed, no standard/guidance of questions available, proposing to create such a common guidance in intacs safety working group
- Assessor with knowledge of all standards or multiple assessors needed - alignment is crucial
- As FUSA and CS request the management of processes, Level 3 of ASPICE is needed for judgement
- Organizational management system audit and project audits are necessary
- Challenge also for the auditee to answer in all three directions - therefore consider onsite audits
- We see advantages as the auditee saves time, but there is a need for preparation:
  - Tooling with the capabilities to map/integrate the three models and the creation of three separate reports
  - preparation and alignment for interviews
  - FUSA & CS manager available within all the interviews to support the domain specialists


Infineon

We deliver

Our solutions span the environmental, social and governance (ESG) spectrum to increase safety, security and sustainability

PEOPLE. PLANET. TRUST.

Certification

Verification

Testing

Auditing and inspection

Software

Data insights

Advisory

Learning and development

We would like to ask the following questions

- Is there a tool from VDA sys already provided for such surveys

- Slide 4: Interactive question: Who is from ASPICE, FuSa, CS
- Slide 6: Interactive question: What is your typical amount of re-assessments
- Slide 12: Interactive question: What is your typical approach for several standards
  - Answers: Separate assessment/audit; partly integrated and reuse of existing reports, fully combined approach


Infineon