Case study

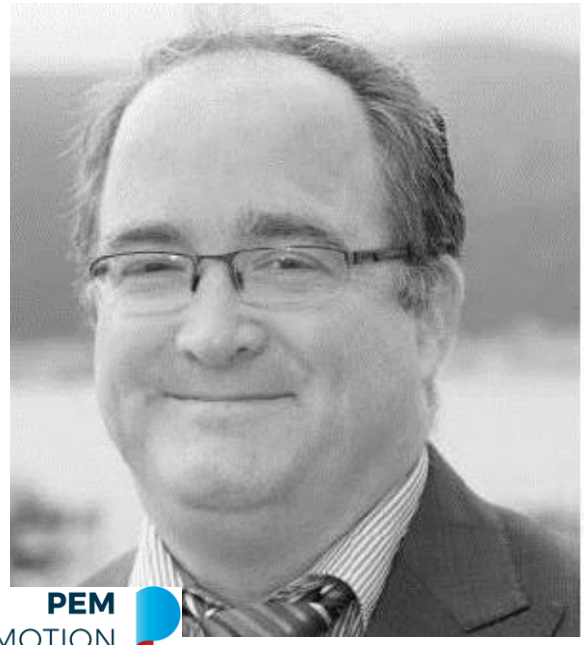
Automotive Spice extension with functional safety and application of Agile-Spice 1.3

SCSSS Scandinavian Conference for System Safety Software 2024

Mark Hirche and Micael Wintsten

COMBITECH PEM MOTION

Who are we?



Mark Hirche

Competent Automotive Spice Assessor since 2024

Working at PEM Motion since June 2024

Previously Lead Safety Assessor at Volvo Trucks (2019...2024)

20+ years of experience within Automotive

Micael Wintsten

Principal Automotive Spice Assessor since 2011

Working at Combitech since 2021

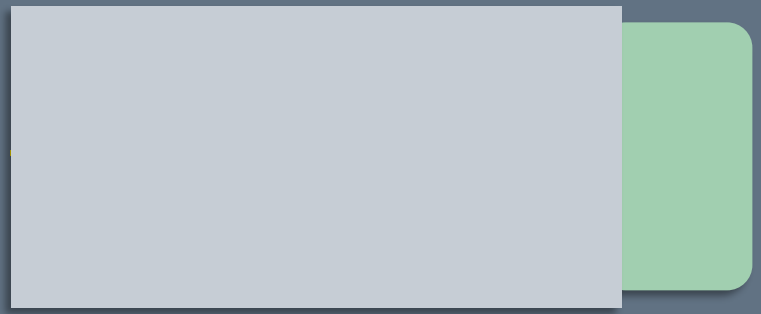
25+ years of experience within Automotive

25+ years of working with system safety

Presentation Content:

- Challenges Ahead
- Model Based Forward looking Assurance Cases
- Tools for Assurance Cases
- The process argumentation: Combination of Automotive Spice and Functional Safety

Challenges ahead



COMBITECH PEM MOTION

The way ahead…

Automotive EE-systems must **meet regulatory requirements for cybersecurity** (UN ECE R-155) and need to comply to **safety and security standards** that define best engineering practices (*ISO 26262 & ISO/SAE 21434*)

At the same time, the whole automotive industry is now rapidly **transitioning to a Continuous Integration / Continuous Deployment** way of developing software/systems.

The continuous integration and deployment process of **new software versions must be lifted from software-level to system-level** and people from different engineering disciplines must be involved.

Applying agile development and the concepts of **continuous delivery** in context of functional safety and cybersecurity requires **to solve specific challenges**. Old practices based on a big bang for SOP/J#1 will not work.

Each delivery of a **new software** to the vehicles **with a potential safety / cybersecurity impact needs to be accompanied with** a consistent and assessed **safety/cybersecurity case**.

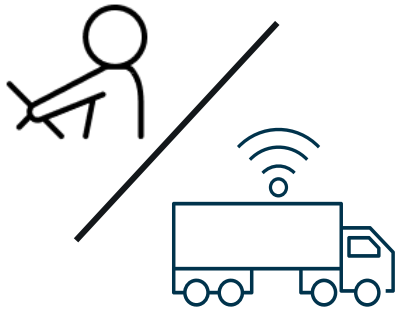
With more and more automated driving tasks with the driver out of the loop **each incident/accident/ cyber attack will be scrutinized to judge if it is caused by bad luck or bad design**.

For this a **well-structured assurance case underpinned with evidence** consistent with the product **will be crucial**.

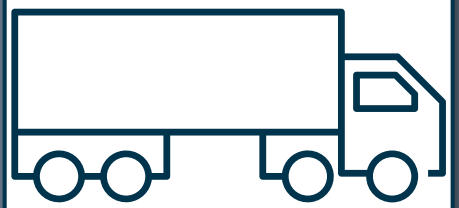
PEM COMBITECH MOTION

If an accident occurs with a truck, what is likely the cause?

Truck Driver



Truck



Road Infrastructure

Other Road Users

PEM COMBITECH MOTION

Manually Driven Truck

- Distracted driving.
- Driving while fatigued.
- Failing to adjust driving to road and weather conditions.
- Driving under the influence of alcohol or drugs.
- Speeding and driving recklessly.
- Negligent hiring by the truck company.
- Failing to properly traindrivers.
- Failing to maintain trucks to a quality standard.
- Failing to observe or enforce the break periods of drivers.
- Reckless driver

Driver Behaviour

Truck Design or Maintenance

Outside of control of the driver

OEM's Expected Liability

PEM COMBITECH MOTION

Autonomously Driven Truck

- Flaws in perception
- Flaws in localization
- Flaws in prediction
- Flaws in path planning
- Flaws in actuation requests
- Etc.

Autonomous Driver

Truck Design or Maintenance

Karma

OEM's Expected Liability = Due Diligence = Safety Case

PEM COMBITECH MOTION

Model Based Forward Looking Assurance Case

Solution and how to argue

COMBITECH PEM MOTION

Assurance Cases – How to use them

An assurance case is used to demonstrate that a system exhibits some complex emergent property such as **safety, security, resiliency, reliability, or survivability**.

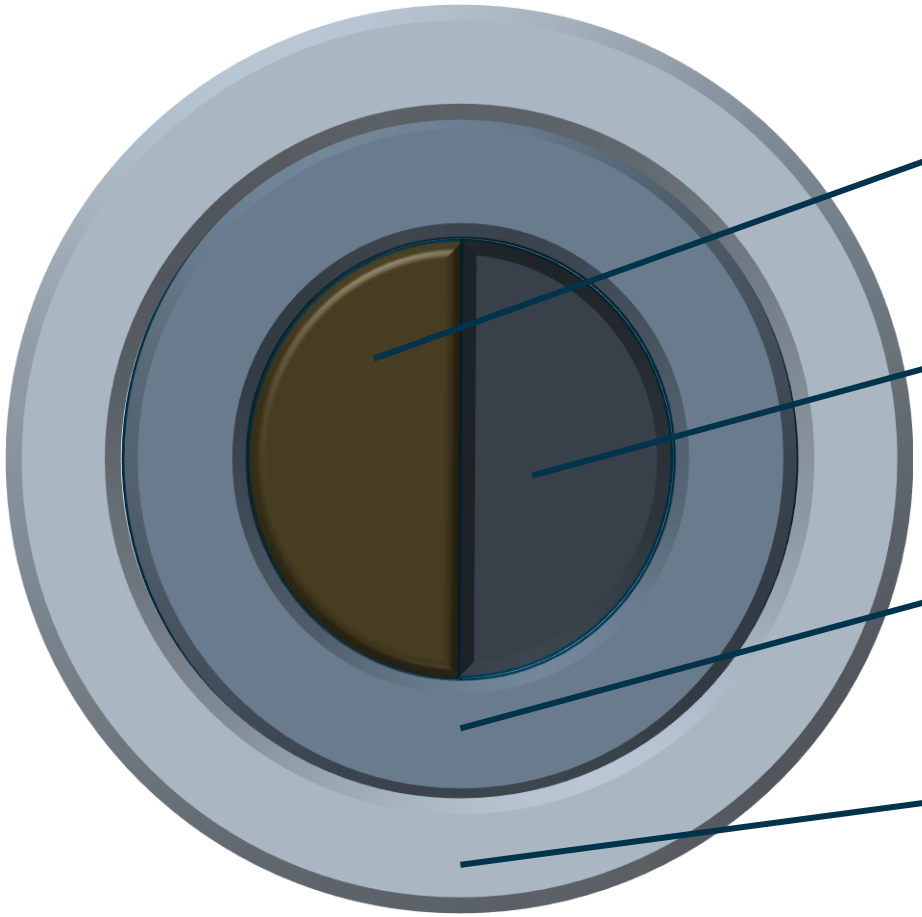
An effective assurance case contains foundational **claims** that are **derived from stakeholder's objectives, credible and relevant evidence** that substantiates the claims, and valid arguments that relate the various evidence to the supported claims.

The **result provides a compelling statement that adequate safety or security** has been achieved and driven by stakeholder needs and expectations.

- Information
  - Claim 0: Functional safety of the realization of <specific End User Function> is achieved
    - Argument 0: Achievement of Functional Safety
      - Rationale
      - Claim 1: The performed work is adequate with respect to functional safety
        - Argument 1: adequate work with respect to functional safety
          - Rationale
          - Claim 1.1: Overall process applied and tools used are adequate
            - Argument 1.1: process and tools are adequate
              - Rationale
              - Claim 1.1.1: Our defined functional safety process is adequate and is being followed
                - Argument 1.1.1: adequate functional safety process
                  - Rationale
                  - Evidence 1.1.1.1: Volvo Group Management System
                    - ISO9001 Process Audit Results
                    - MIRA FSMS Audit Results
                  - Evidence 1.1.1.2: Functional Safety Audit Reports
                    - ASPICE SS7740 Audit Result
              - Claim 1.1.2: Our quality management procedures are adequate and are being applied
                - Argument 1.1.2: Adequate QM
                  - Rationale
                  - Evidence 1.1.2: Evidence of quality management
              - Claim 1.1.3: For software development, guidelines for coding, modelling, integration and use of tools exist and are applied
                - Argument 1.1.3: Guidelines for software development exist and are used
                  - Rationale
                  - Evidence 1.1.3.1: Guidelines
                  - Evidence 1.1.3.2: Evidence that guidelines have been followed
              - Claim 1.1.4: Tools used are adequate
                - Argumentation 1.1.4: Adequate Tools
                  - Rationale
                  - Evidence 1.1.4.1: Software Tool Criteria Evaluation Report
                  - Evidence 1.1.4.2: Software Tool Qualification Report
          - Claim 1.2: Adequate in-house competence and safety culture is ensured
            - Argument 1.2: Adequate in-house competence and safety culture
              - Rationale
              - Evidence 1.2.1: Evidence of competence and safety culture in organisation
              - Evidence 1.2.2: Project-specific competence evidence (in Technology Project Description or dedicated safety plan)

PEM COMBITECH MOTION

How does a structured argument look like - MISRA Safety Case Model



Core argument 1 (Rationale):
- Argument that the requirements are right.
- Evidence from HARA/TARA, FSC/TSC indicating that the requirements are complete and correct.

Core argument 2 (Satisfaction):
- Argument that the requirements have been implemented correctly (satisfied).
- Evidence from verification indicating the correct implementation.

Layer 1 argument: (Means)
- Argument that an adequate process has been used in the development of the product
- Evidence demonstrating that the right people have used the correct methods.

Layer 2 argument: (Environment)
- Argument over an environment that promotes safety activities (organisational context).
- Evidence demonstrating that the organization has a good safety culture.

PEM COMBITECH MOTION

Tools for Assurance Cases

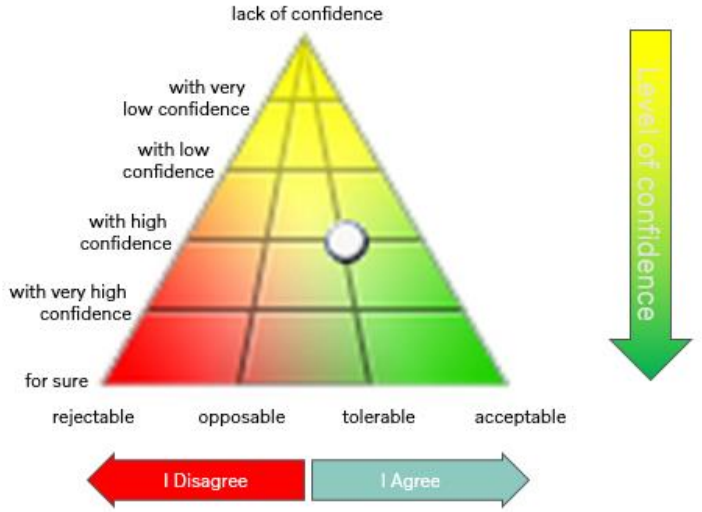
Our choice and the motives behind

COMBITECH PEM MOTION

Utilizing Forward-looking Assurance Cases

Excerpt from ISO 26262-2:2018

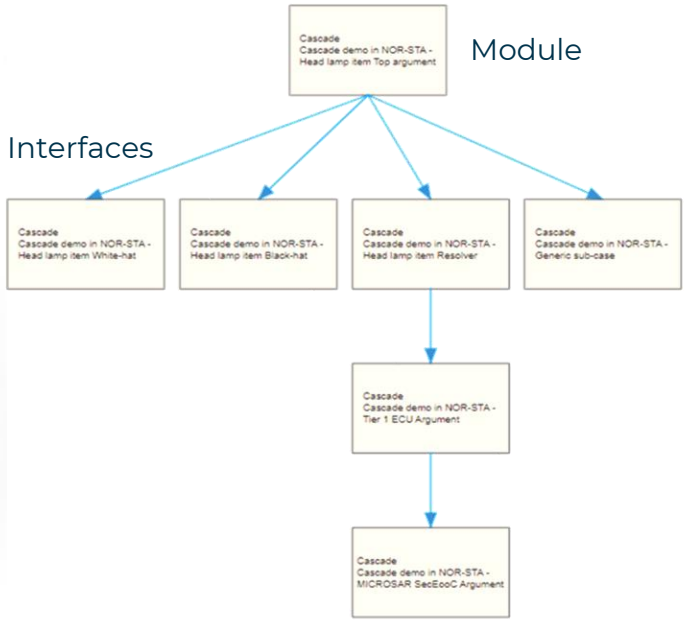
> NOTE 2 To support safety planning according to 6.4.6, the intended safety arguments can be identified prior to work products becoming available. To support progressive functional safety assessments according to 6.4.12.3 the safety case can be released progressively as work products are generated to provide evidence for the safety arguments.



- The safety argumentation is developed in advance to constitute a goal and an agreement between team and assessor
- By executing the required processes the agreed evidence is produced to underpin the argument
- The argument is progressively assessed and the results is presented as a model of the assessor's confidence in the argument.

Through Modular Assurance Cases each team brings their piece of the assurance case

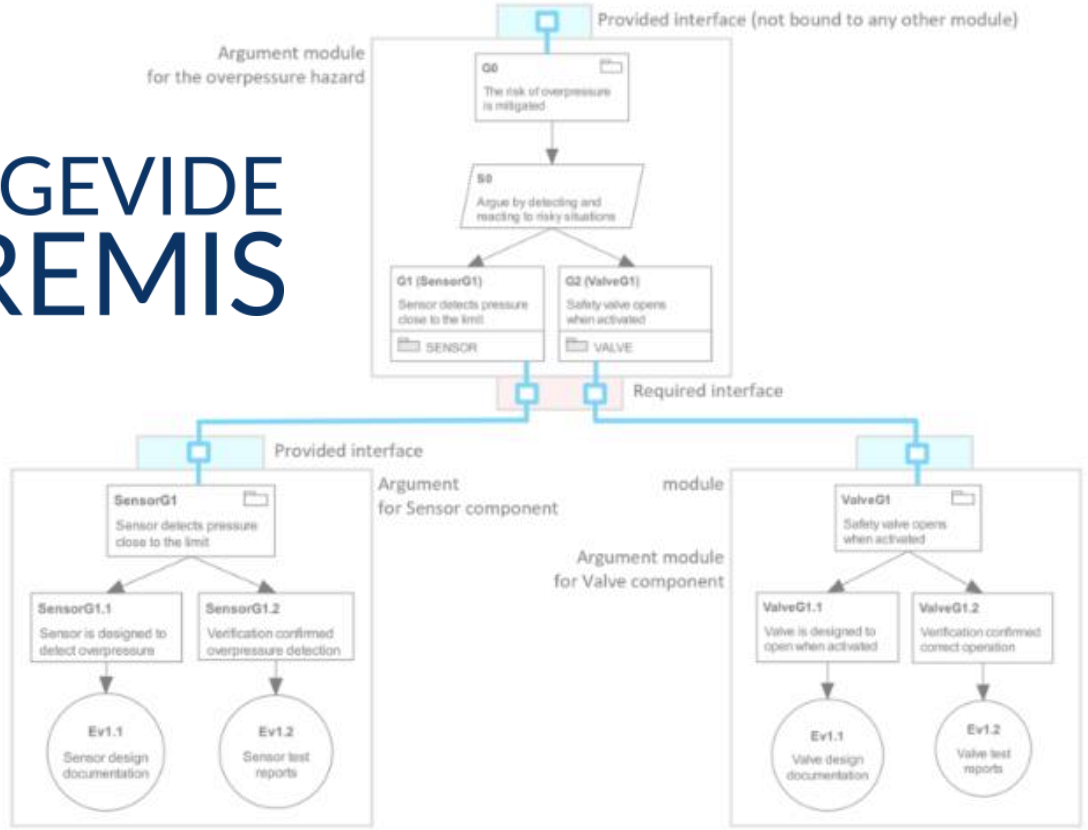
Assurance Case Architecture



PEM COMBITECH MOTION

Tools that can be used

ARGEVIDE PREMIS



PEM COMBITECH MOTION

The process argumentation: Aspice and Functional Safety

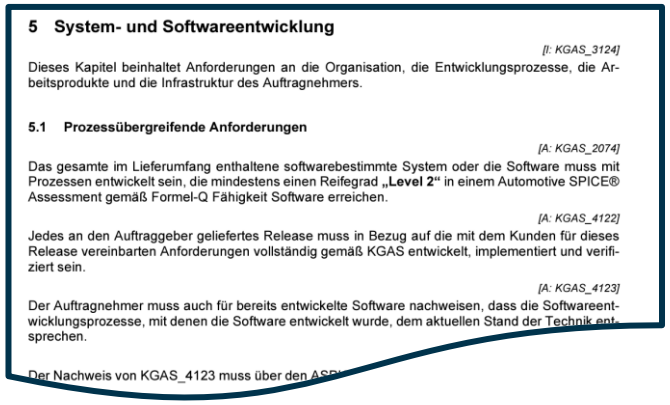
Using SS7740 for Process Maturity Measurement

COMBITECH PEM MOTION

OEM requirement for mechatronic products and Quality Improvement

Volkswagen

- Level 2



5 System- und Softwareentwicklung

[I: KGAS_3124]

Dieses Kapitel beinhaltet Anforderungen an die Organisation, die Entwicklungsprozesse, die Arbeitsprodukte und die Infrastruktur des Auftragnehmers.

5.1 Prozessübergreifende Anforderungen

[A: KGAS_2074]

Das gesamte im Lieferumfang enthaltene softwarebestimmte System oder die Software muss mit Prozessen entwickelt sein, die mindestens einen Reifegrad **„Level 2"** in einem Automotive SPICE® Assessment gemäß Formel-Q Fähigkeit Software erreichen.

[A: KGAS_4122]

Jedes an den Auftraggeber geliefertes Release muss in Bezug auf die mit dem Kunden für dieses Release vereinbarten Anforderungen vollständig gemäß KGAS entwickelt, implementiert und verifiziert sein.

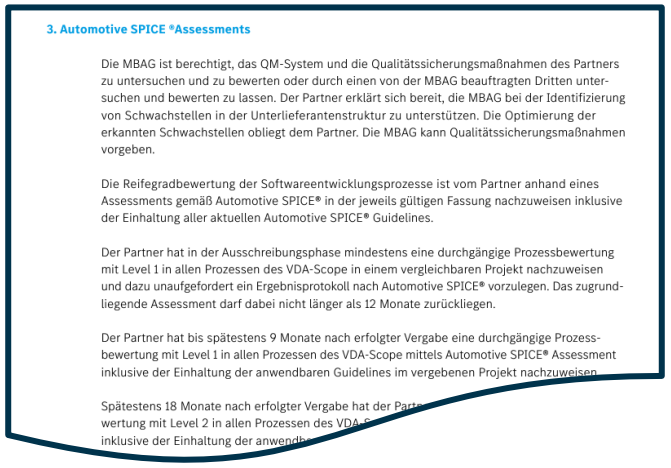
[A: KGAS_4123]

Der Auftragnehmer muss auch für bereits entwickelte Software nachweisen, dass die Softwareentwicklungsprozesse, mit denen die Software entwickelt wurde, dem aktuellen Stand der Technik entsprechen.

Der Nachweis von KGAS_4123 muss über den ASP

Mercedes Benz

- RFQ: Level 1
- R&D: Level 2



3. Automotive SPICE ®Assessments

Die MBAG ist berechtigt, das QM-System und die Qualitätssicherungsmaßnahmen des Partners zu untersuchen und zu bewerten oder durch einen von der MBAG beauftragten Dritten untersuchen und bewerten zu lassen. Der Partner erklärt sich bereit, die MBAG bei der Identifizierung von Schwachstellen in der Unterlieferantenstruktur zu unterstützen. Die Optimierung der erkannten Schwachstellen obliegt dem Partner. Die MBAG kann Qualitätssicherungsmaßnahmen vorgeben.

Die Reifegradbewertung der Softwareentwicklungsprozesse ist vom Partner anhand eines Assessments gemäß Automotive SPICE® in der jeweils gültigen Fassung nachzuweisen inklusive der Einhaltung aller aktuellen Automotive SPICE® Guidelines.

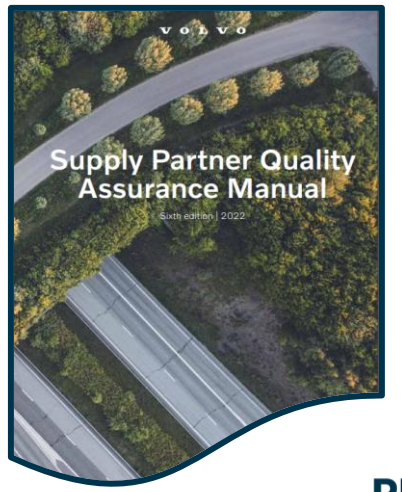
Der Partner hat in der Ausschreibungsphase mindestens eine durchgängige Prozessbewertung mit Level 1 in allen Prozessen des VDA-Scope in einem vergleichbaren Projekt nachzuweisen und dazu unaufgefordert ein Ergebnisprotokoll nach Automotive SPICE® vorzulegen. Das zugrundliegende Assessment darf dabei nicht länger als 12 Monate zurückliegen.

Der Partner hat bis spätestens 9 Monate nach erfolgter Vergabe eine durchgängige Prozessbewertung mit Level 1 in allen Prozessen des VDA-Scope mittels Automotive SPICE® Assessment inklusive der Einhaltung der anwendbaren Guidelines im vergebenen Projekt nachzuweisen.

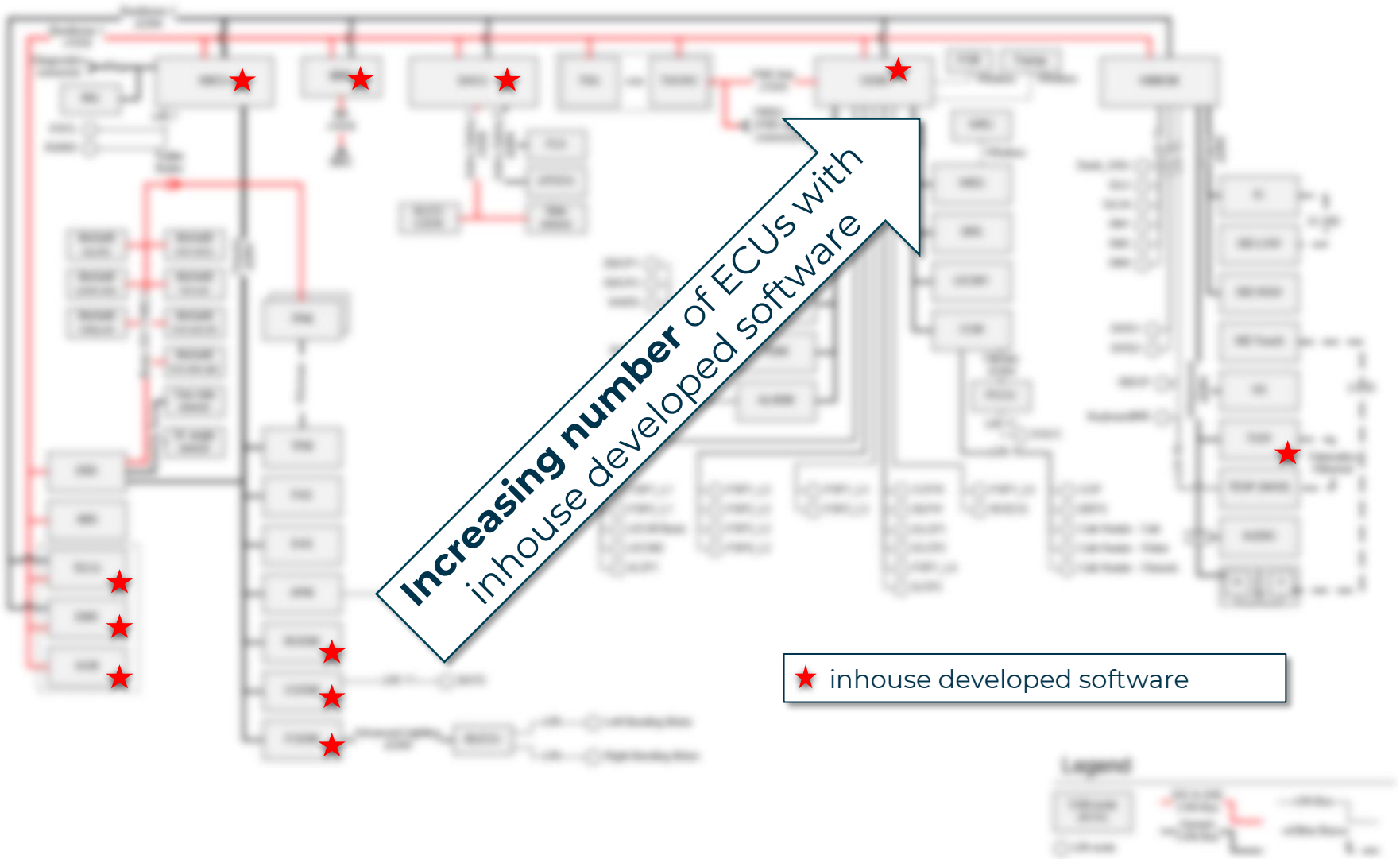
Spätestens 18 Monate nach erfolgter Vergabe hat der Partn
wertung mit Level 2 in allen Prozessen des VDA-S
inklusive der Einhaltung der anwendb

Volvo Group

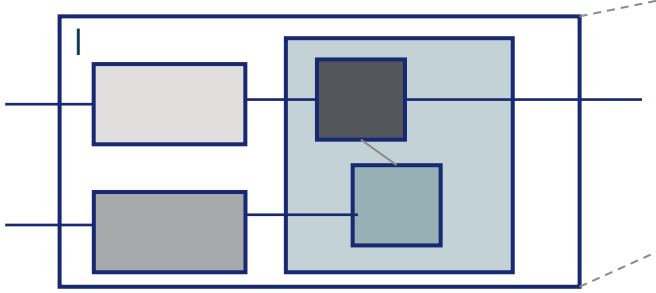
- Level 3
- ASPICE or ISO33000 CL 3 proven by assessment reports by an accredited 3rd party



201X - ...


Increasing number of ECUs with inhouse developed software
inhouse developed software

Why SS7740 ?



FUNCTIONAL SAFETY ASSESSMENT

Overall ”check” that part of the item is safe

relies on

relies on

CONFIRMATION REVIEWS

Checks some of the work products of the (part of) the item

FUNCTIONAL SAFETY AUDIT

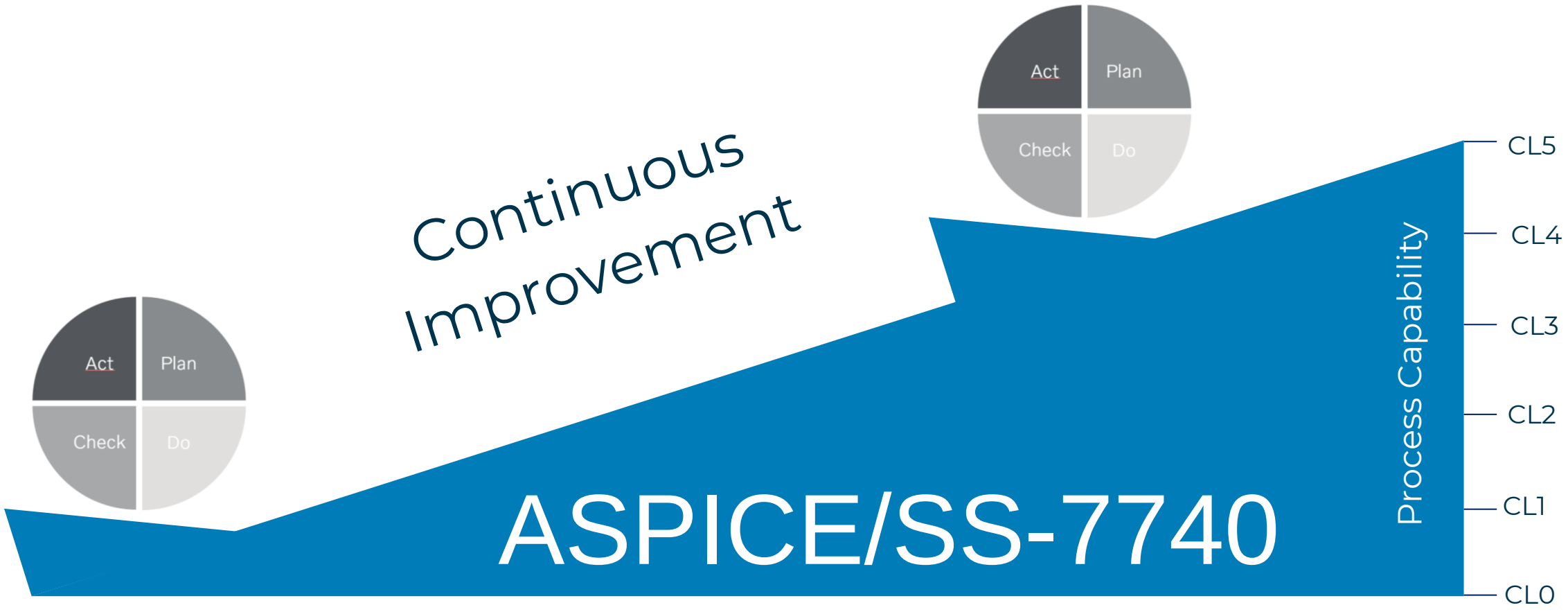
Checks the process capability of the organization

inspects

SAFETY WORK PRODUCTS

ISO 26262, part 2, Clause 6.4.8, Note 1:
If a functional safety audit is performed by a Software Process Improvement and Capability Determination (SPICE) assessor, then this functional safety audit and a SPICE assessment (see ISO/IEC 15504) can be performed simultaneously. There can be sufficient commonality in content between ISO 26262 and SPICE to allow synchronization of the planning. If synchronized, the SPICE assessor can provide feedback to the functional safety auditor. However, a SPICE assessment can only be synchronized with regard to the examination of some of the supporting process specified in ISO 26262-8 and is not sufficient to perform the functional safety assessment (see 6.4.9).

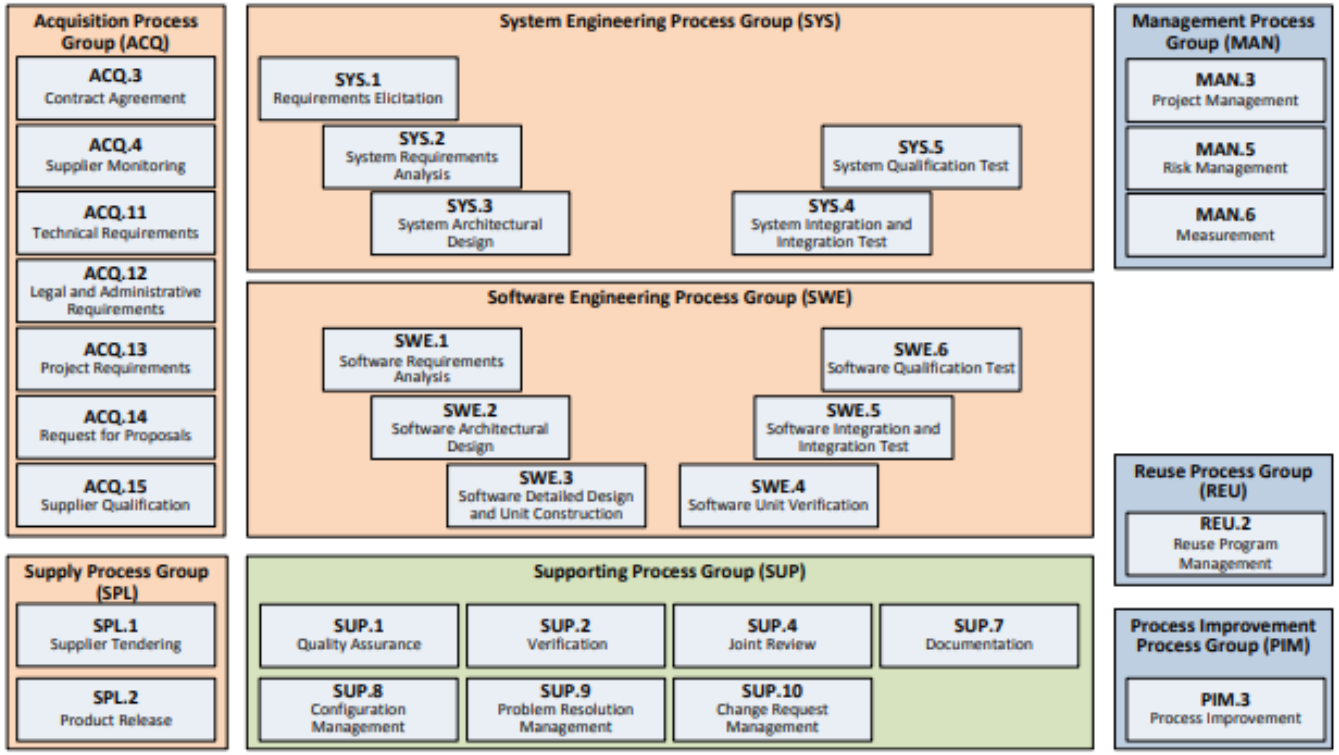
PEM COMBITECH MOTION


Act
Plan
Check
Do
Continuous Improvement
Act
Plan
Check
Do
ASPICE/SS-7740
Process Capability
CL5
CL4
CL3
CL2
CL1
CL0

What is SS7740

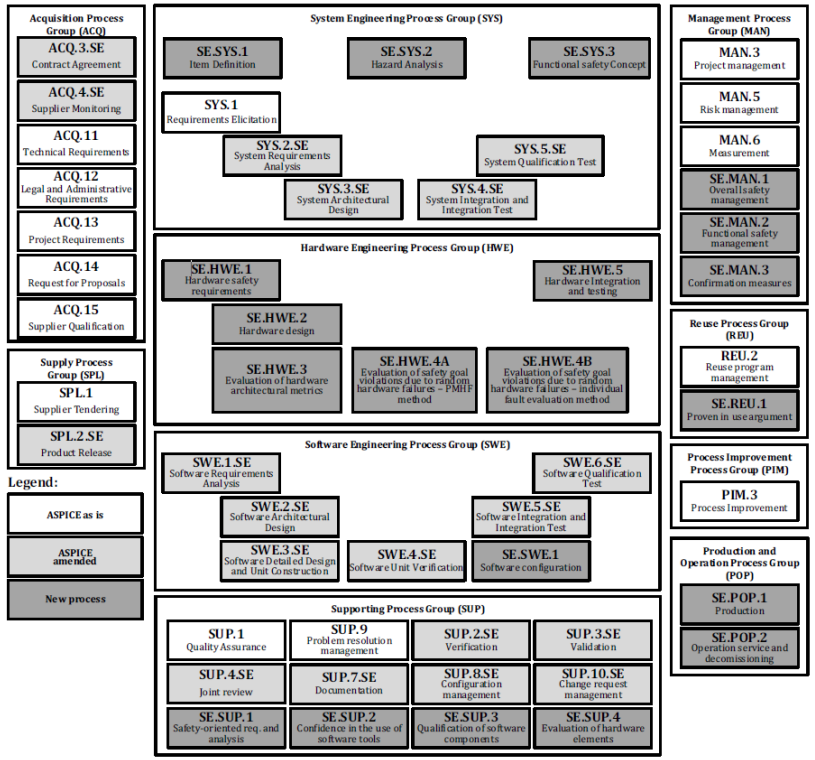
SiS Svenska Institutet för Standarder **SS7740**

Automotive Spice



Extension of ASPICE PRM & PAM for Functional Safety

Used by us as Functional Safety Audit Method



Legend:	**Description:**
ABC	process unchanged from ASPICE
ABC.SE	ASPICE process amended
SE.ABC	new process

PEM COMBITECH MOTION

Our findings when doing the SS7740 process assessments

Including Agile Spice

COMBITECH PEM MOTION

The **fully achieved** rated processes are the ones where the departments are making use of

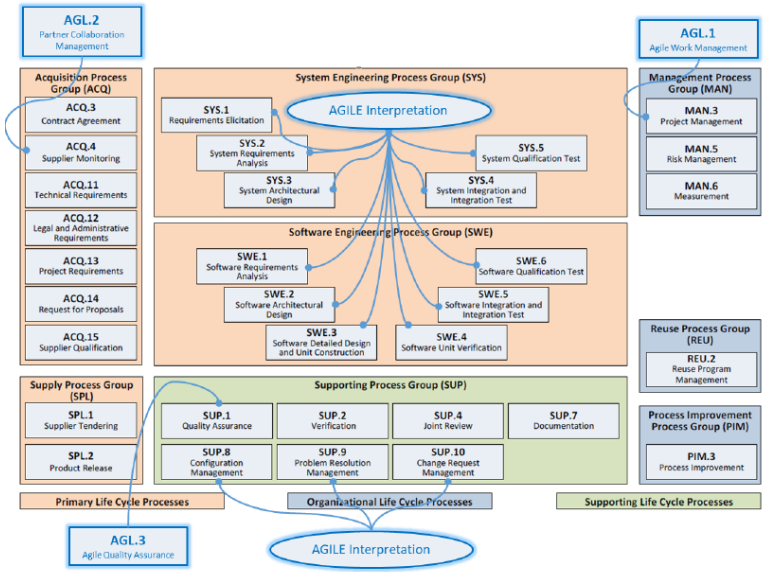
- Mature processes
- Centrally defined

Be careful when doing tailoring

Involve the assessors early

Setup COP to spread learnings

COMBITECH PEM MOTION



The agile aspect

- Due to that the OEM has implemented Scaled Agile on a corporate level there is also the need to consider the effects on process maturity evaluation
- As a result of above we modified the scope of the gap analyses that have been done and included Agile Spice 1.3 into the scope without removing the ASPICE general management, acquisition and supporting processes (means MAN.3, SUP.1, etc.).

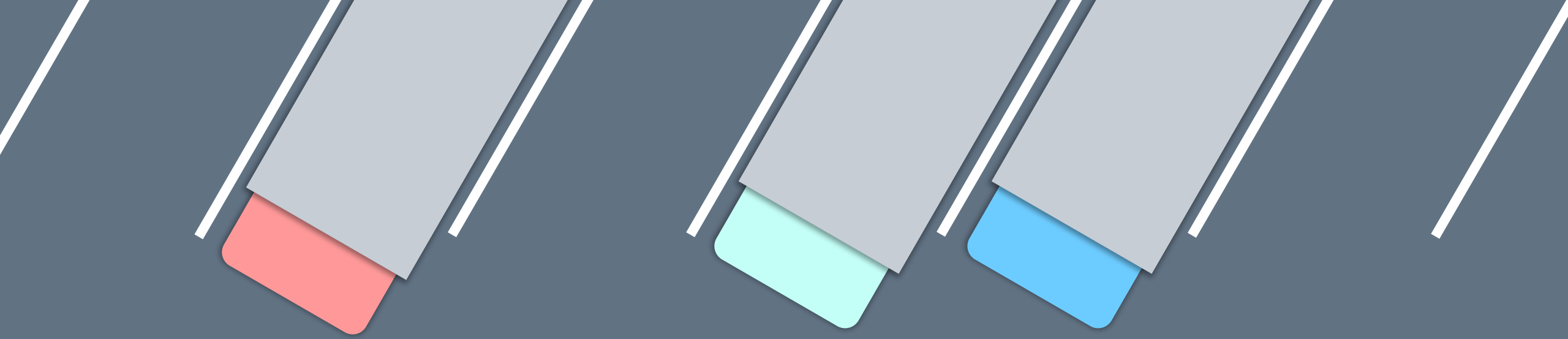
Missing aspects

- Our feeling regarding agile SPICE improvement potential lies in the separation of work-product and process quality assurance.
- The standard Automotive SPICE has strengths in giving more hands-on assessment guidelines
- Agile SPICE contains the risk of focus on work-product quality assurance.

Mapping of language

- A very positive aspect of agile SPICE is the usage of terminology which is known in the organisation due to the company-wide introduction of Safe Agile.
- This modernization of language used was taking away hinders like people thinking that aspice is old fashioned and not possible to apply in an agile context.

COMBITECH PEM MOTION

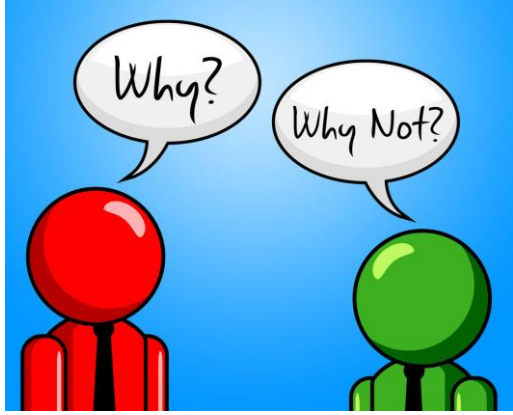


Conclusions and what happens next

COMBITECH PEM MOTION

Conclusions

- There is an increasing need of argumentation for application of adequate processes which is used in assurance cases – we see the SPICE-PAMs as an invaluable tool in achieving the argumentation
- As OEMs are putting requirements onto the supply chain of up to ASPICE Level 3, also OEMs need to have a sufficient maturity level of the product development processes so that the confidence of the process argumentation is not endangered.
- SS7740 is a powerful tool that does gives answers on process capability stretching over ISO26262, as ASPICE processes got amended/completed
- Potential of adding additional models like Mechanical SPICE, etc. – synergy

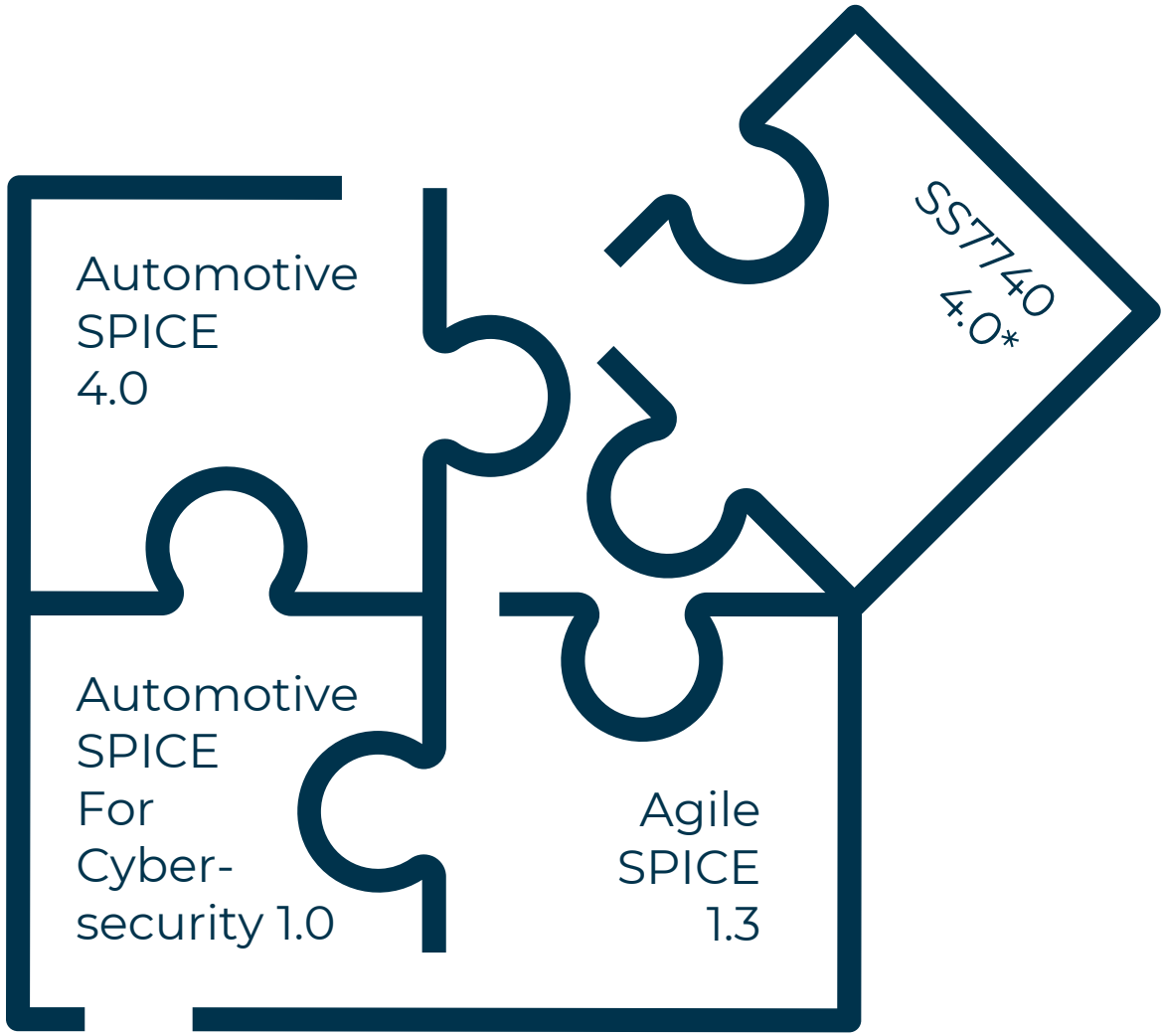


- Independent of the process maturity start the evaluation early to find improvement potential.
- Continuous improvement aspect is important to not de-motivate the organisation, but rather strengthen the eagerness to improve – the mindset is important !
- Give time to improve, without removing the urgency of process maturity improvement

Using SS7740 in combination with other PAMs is an efficient way to find process arguments that are objective for your assurance case.

What happens next

- Work is ongoing to synchronize SS7740 to the Automotive Spice Framework 4.0, which has changed to a Plugin Concept, whereas SS7740 was written with a ”can be used as it is”-attitude
- Synchronisation with the intacs working group has not been fruitful as of now, there seems to be a ”not-invented-here” attitude
- As SS7740 is used in sweden not only at one company there is a benefit of keeping it up-to-date and transforming it into an ISO at a later stage.
- That SS7740 is a valuable tool has been proven in several areas.



* Working Title

Example: Process Development Usage

For companies aiming at innovative products

SMART HOUSING by HOERBIGER

Wireless Communication

Networking via Bluetooth LE

- **Replacement of low voltage wiring harness and bonding**
- **Enabler for new vehicle architectures**
- **Re-use / easier module exchangeability**

Enhanced Sensors

Measuring of temperature, voltage and pressure on cell level

- **EIS measurement (optional)**
- **Higher charging rate**
- **Expanded operation range**
- **Efficient thermal management**

On-Cell Diagnosis

SoH determination on cell level

- **Damage detection in case of an accident**
- **Improved determination of residual value**
- **Passive balancing**

Data Storage

Data mining over lifetime for

- **Battery pass**
- **Re-Use applications**
- **Benefits from process optimization end of line & begin of line process steps**
  - **Grading, Aging, Sorting**

We are offering

PEM Motion support in:

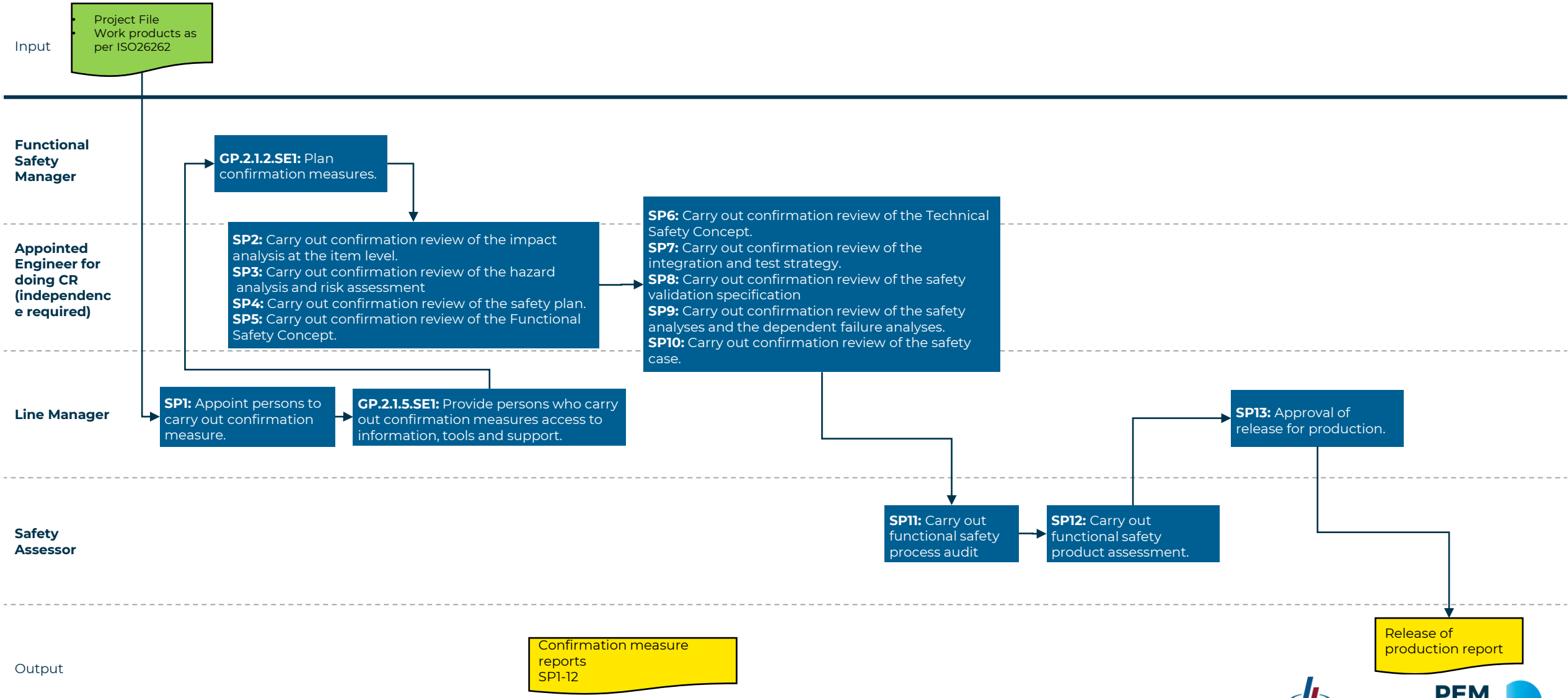
- Process Development and Improvement
- Concept Development
- Functional Safety
- Cybersecurity

One of the tools:

- SS7740:2023

HOERBIGER PEM MOTION

Example: SE.MAN.3 Confirmation Measures



Example: Role Description Functional Safety Assessor

Responsibility:

- Carry out functional safety process and product assessment for all projects and products that require assessment
- Carry out confirmation review according ISO 26262:2018 for all work products (that require an independence level of i2 and above)

Competency:

- min. Bachelor Degree plus relevant Experience or a Masters Degree in an Engineering Discipline (Data Science, Electrical Engineering, or similar)
- min. 15 years of experience in Automotive Development
- Automotive Functional Safety Background (min. participation in one safety related project from concept to industrialization phase)
- extensive experience of doing confirmation reviews all along the lifecycle

Knowledge:

- Functional Safety Certification is meritorious, but in detail knowledge of the ISO26262 and interpretation is needed
- Assurance Case knowledge and experience with claim/evidence argumentation is needed
- quality assurance (APQP/PPAP/…) experience is needed
- quality tool (FMEA/FTA/Markov) application experience needed
- excellent communication skills
- assessment- and auditing skills are necessary

BAE SYSTEMS

Hägglunds AB

Picture: CV90

Combitech supports BAE Systems Hägglunds in:

- Product Development
- System safety
- Process Development and Improvement

One of the tools:

- SS7740:2023

COMBITECH

alfdex®

Combitech supports Alfdex in:

- System safety
- Process Development and Improvement
- Supplier management

One of the tools:

- SS7740:2023

 · Case study

COMBITECH

Where to get the PAMs:

SS7740:2023

Svenska Institutet för Standarder

https://www.sis.se/

ASPICE Rel. 3.1

AUTOMOTIVE SPICE®

https://www.automotivespice.com/

Agile SPICE Rel. 1.3

intacs.info

International Assessor Certification Scheme

https://intacs.info/

Q&A

COMBITECH PEM MOTION