Experience Report from Recent Combined Assessments: ASPICE 3.1 + ISO 26262

TechDay 30.8. , and EuroSPI, 1.-3.9.2021

Experiences from ISCN

Suported by By SOQRATES Group https://soqrates.eurospi.net

We make your safety audit and assessment work in practice

Presenter Researcher Profile

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

Motivation

(1) Strategy until 2019: Safety Audit overlaps with ASPICE Assessment

- ASPICE questionnaire with extended questions
- Only remaining non overlapping topics (e.g. part 7 safety norm for production) asked extra

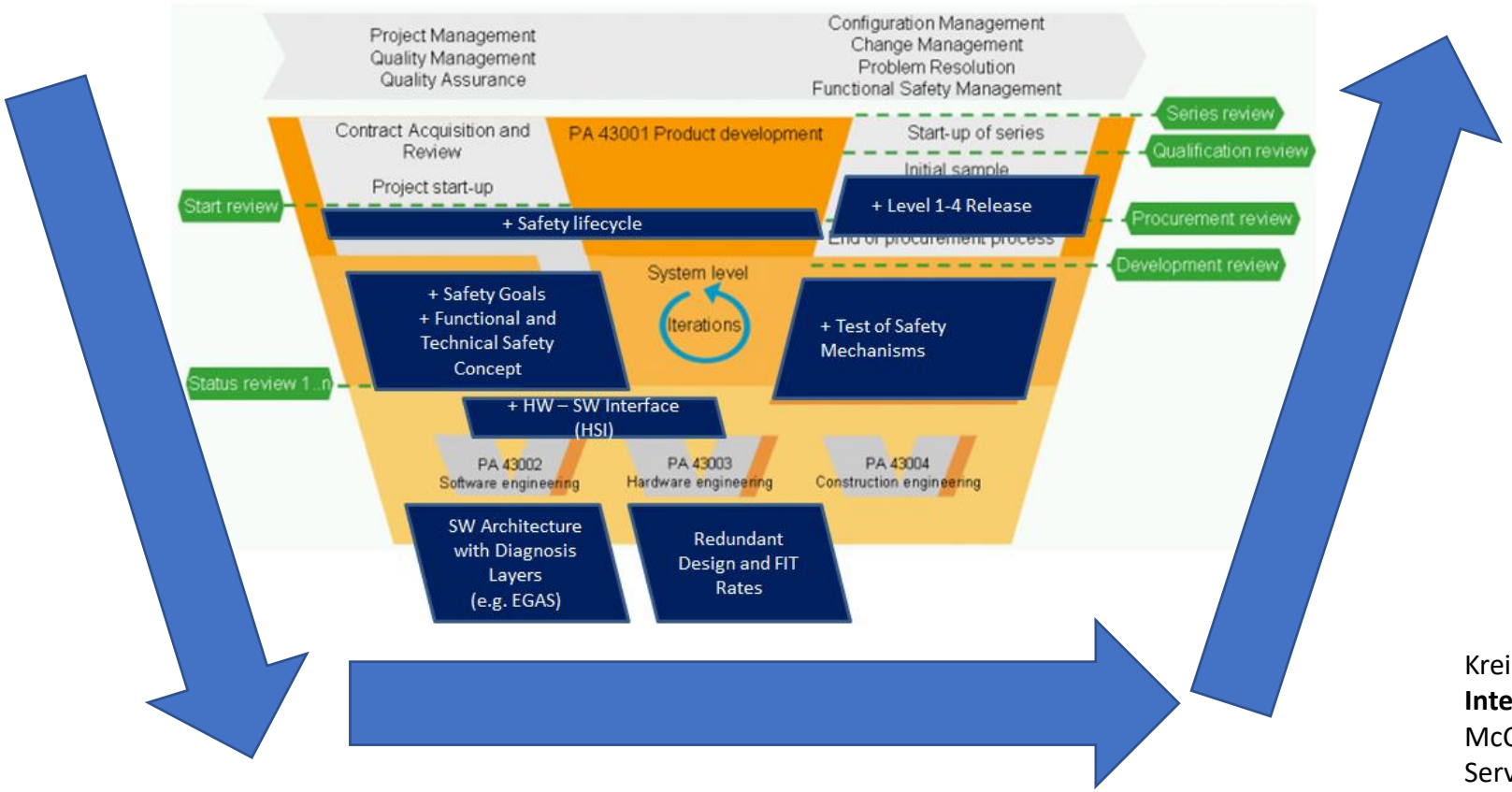
(2) New Strategy from 2020/2021 (already implemented in e.g. Daimler, BMW etc. projects by ISCN)

- Invention of a safety assessment technique that is aligned with the ASPICE V and walks in detail / technically through the safety goals (the most critical ones full technical check and the remaining by technical review)

Conclusion

- (1) allowed a combination of the safety audit. (2) offers a new approach to run the safety assessment in a structured V approach per safety goal. (3) Both can be combined in one strategy.

Approach



- ✓ Check per Safety Goal
- ✓ Technical Review along V Model
- ✓ Traceability of the safety case
- ✓ Work Products related will be checked

Kreiner C. et al. (2013) **Automotive Knowledge Alliance AQUA – Integrating Automotive SPICE, Six Sigma, and Functional Safety**. In: McCaffery F., O'Connor R.V., Messnarz R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2013. Communications in Computer and Information Science, vol 364. Springer, Berlin, Heidelberg

Safety Assessment of Safety Goals

Detailed Technical Check of work products content per safety goal

SystemV & SW V & HW V

Interview block x (x = 1 ..3)

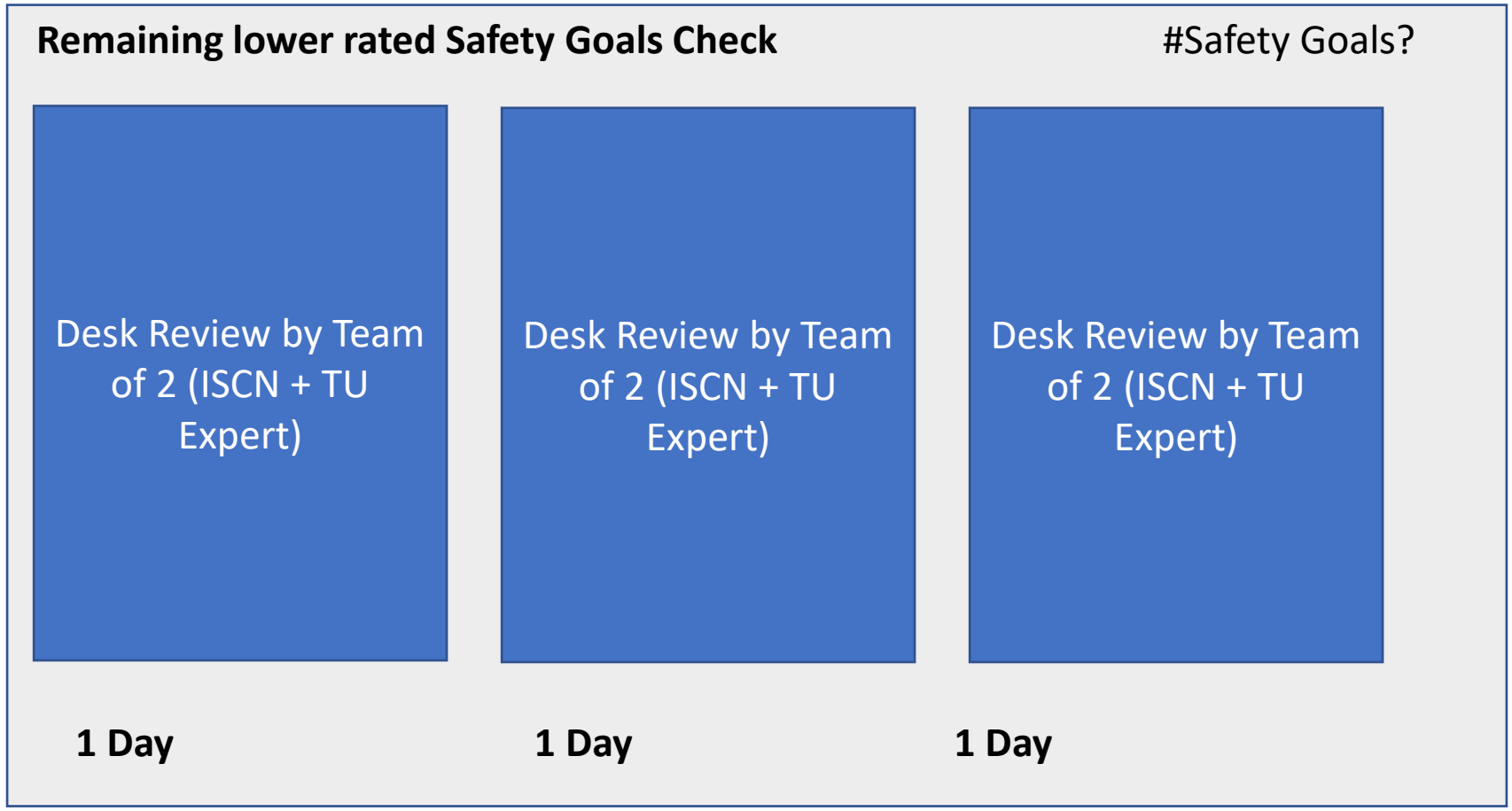
Safety Goal x – For each of the Highest/Most Critical 3 Safety Goals 1,5 days

System V ASPICE+	SW V ASPICE +	HW V HW SPICE+
Safety Goals Technical Safety Concept Hardware SW Interface ASIL Decomposition / DFA Safety Critical Signal Flow Related Safety Reqs. ASIL classified System Design Components and Interfaces Safety Test Cases Safety Test Reports Safety Coverage Metrics	SW Safety Analysis / SW FMEA ASIL classified SW Components ASIL classified SW interfaces Safety Critical Signal Flow Freedom from Interference Safety Critical Monitoring and Diagnose Functions Base Software Complex Driver CPU Firmware eval. Of SEooC Manual Safety Test Cases Safety Test Reports Safety Coverage Metrics	HW Safety Analysis / HW FMEA ASIL classified HW Module ASIL classified HW interfaces Safety Critical Signal Flow on HW Freedom from Interference FMEDA HW Architecture Metrics FIT and Diagnostic Coverage HW Safety Test Cases HW Safety Test Reports HW Safety Coverage Metrics
½ Day	**½ Day**	**½ Day**

Even if we check work products we enter the deviations in the assessment tool with marker WP assessment.

!

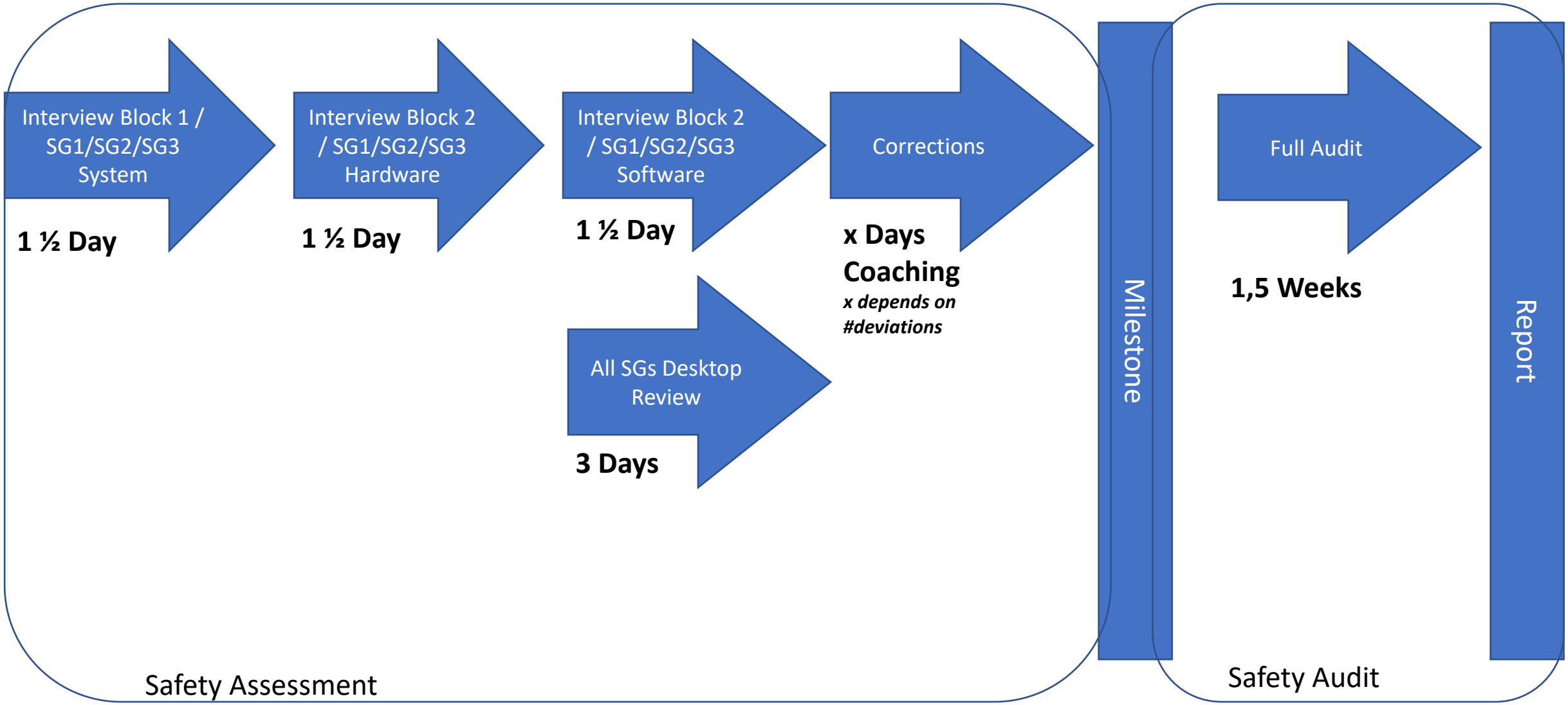
Review of Remaining Safety Goal in Home Office by Experts



Even if we check work products we enter the deviations in the assessment tool with marker WP assessment.

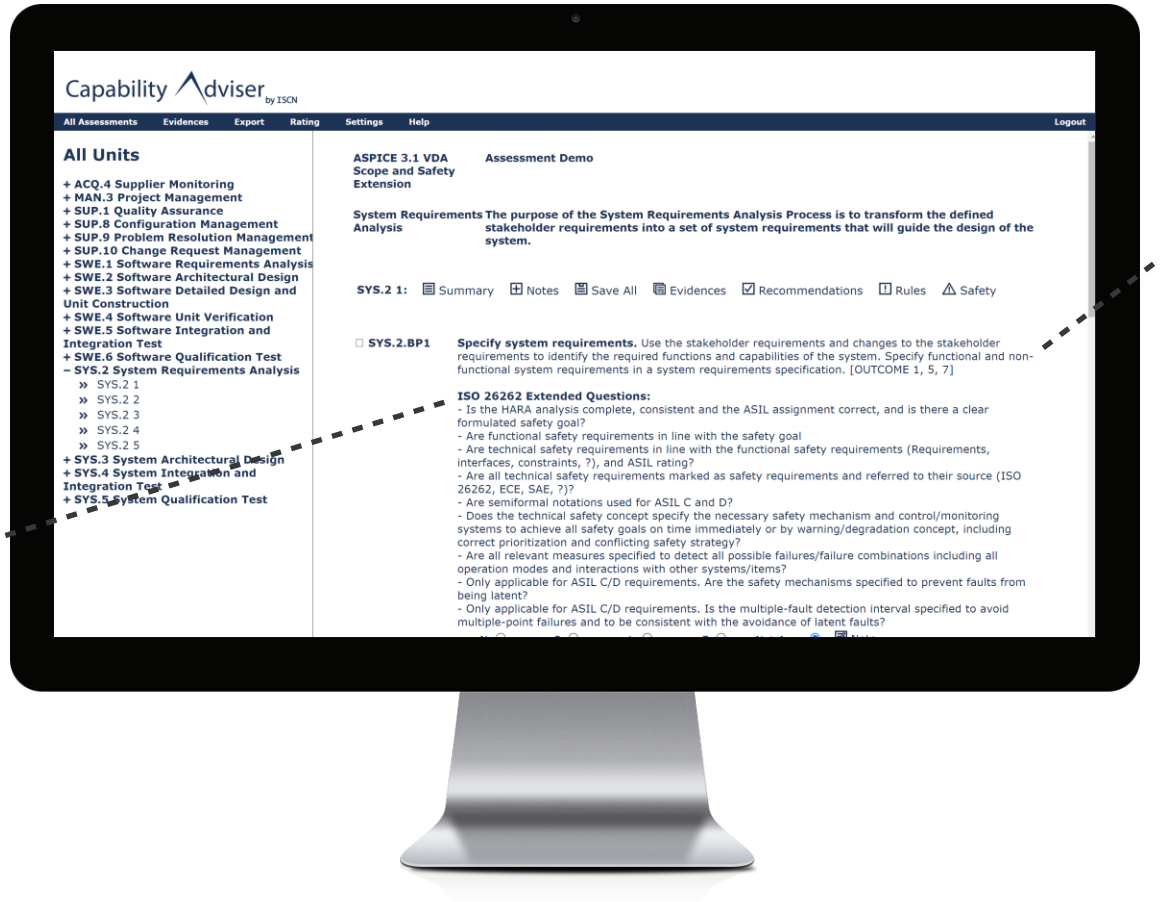
!

Generic Schedule



FUNCTIONAL SAFETY & AUTOMOTIVE SPICE

A unique Integrated Automotive & Safety SPICE Assessment Approach.



Extended Base and Generic Practices

Switch between Automotive SPICE and Safety Scope

Different Ratings depending on the Scope for the same Practice

Capability Adviser by ISCN

All Assessments | Evidences | Export | Rating | Settings | Help | Logout

All Units

+ ACQ.4 Supplier Monitoring
+ MAN.3 Project Management
+ SUP.1 Quality Assurance
+ SUP.8 Configuration Management
+ SUP.9 Problem Resolution Management
+ SUP.10 Change Request Management
+ 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
+ SYS.2 System Requirements Analysis
− SYS.3 System Architectural Design
  - » SYS.3 1
  - » SYS.3 2
  - » SYS.3 3
  - » SYS.3 4
  - » SYS.3 5
+ SYS.4 System Integration and Integration Test
+ SYS.5 System Qualification Test

ASPICE 3.1 VDA Scope and Safety Extension **Safety Extension of ASPICE Demo**

System Architectural Design **The purpose of the System Architectural Design Process is to establish a system architectural design and identify which system requirements are to be allocated to which elements of the system, and to evaluate the system architectural design against defined criteria.**

SYS.3 1: Summary | Notes | Save All | Evidences | Recommendations | Rules | Safety

☑ **SYS.3.BP1** **Develop system architectural design.** Develop and document the system architectural design that specifies the elements of the system with respect to functional and non-functional system requirements. [OUTCOME 1]

ISO 26262 Extended Questions:
- Show a technical safety concept including not only requirements but a technical safety architecture
- Show the decomposition/redundancy strategy depending on the assigned ASIL levels.
- Design of hardware based on safety requirements and required fit rates and redundancies. The safety-relevant hard- and software parts and safety functions are identified and marked.
- Consider the entire functional flow starting from the sensors to the ECU. Show the signal flow to reach a safe state (including the overall hardware and software, sensors, actuators, programmable electronics, etc). Include timing aspects like latency time, reaction time.
- Design exception handling and diagnose system on different levels which for each critical error switches to a control state. Consider diagnose levels and use the e-gas model as a reference case. (Level 1 - base diagnosis, Level 2 - independent plausibility checks and functional diagnosis, Level 3 - system control, checking the call sequences, processor, etc.).
- Demonstrate the appropriate selection of the processor architecture, the amount of self- diagnose covered by the processor architecture, and the amount of additional control measures needed to protect against processor failures.
- Show how the subsystem requirements (e.g. software safety requirements) are derived from the technical safety requirements/concept and the system design. This needs to be demonstrated in the linking model.
- Show that all operating modes of the system have been considered, and demonstrate the task management, especially for the safety tasks.
- How the coverage of hardware error models (derived from FTA and FMEDA). Define and analyse hardware metrics to assure a safe state in case of random hardware failure to cover hardware diagnostic features to detect random hardware failures, and to select the right hardware solution to reach the target values.
- Treat all the hardware and software as safety-relevant where a safety-relevant system is intended to realize both safety and non-safety functions unless it can be shown that the implementation of the safety and non-safety functions is sufficiently independent (i.e. that the failure of any non-safety-related functions does not affect the safety-related functions).
- Use the ISO 26262 method tables to demonstrate that appropriate system design techniques were used (depending on the ASIL classification)

N ○ P ○ L ◉ F ○ Not App. ○ Note

Strengths:

```
Safety Goal 1 Check - ASIL B:
Figure 2 SYS.3_9322
The Figure 2 shows in yellow and red the signal flow to control temp and if one
of the two is exceeding limit by HW it switches off
Filter for A_SafetyGoal = SG1
12 reqs. are related purely to SG1
Re. ID SYS3_3320 with temp limits 110 - 115 - 120 (range), the limit.
Measurement range 25-150
```

Weaknesses:

```
Safety Goal 1 related:
SYS3_411 the 2 temp sensors should be each ASIL-A, it is QM?, should be A
SYS3_416 the OR gate in the signal path in HW is single point fault possibility,
```

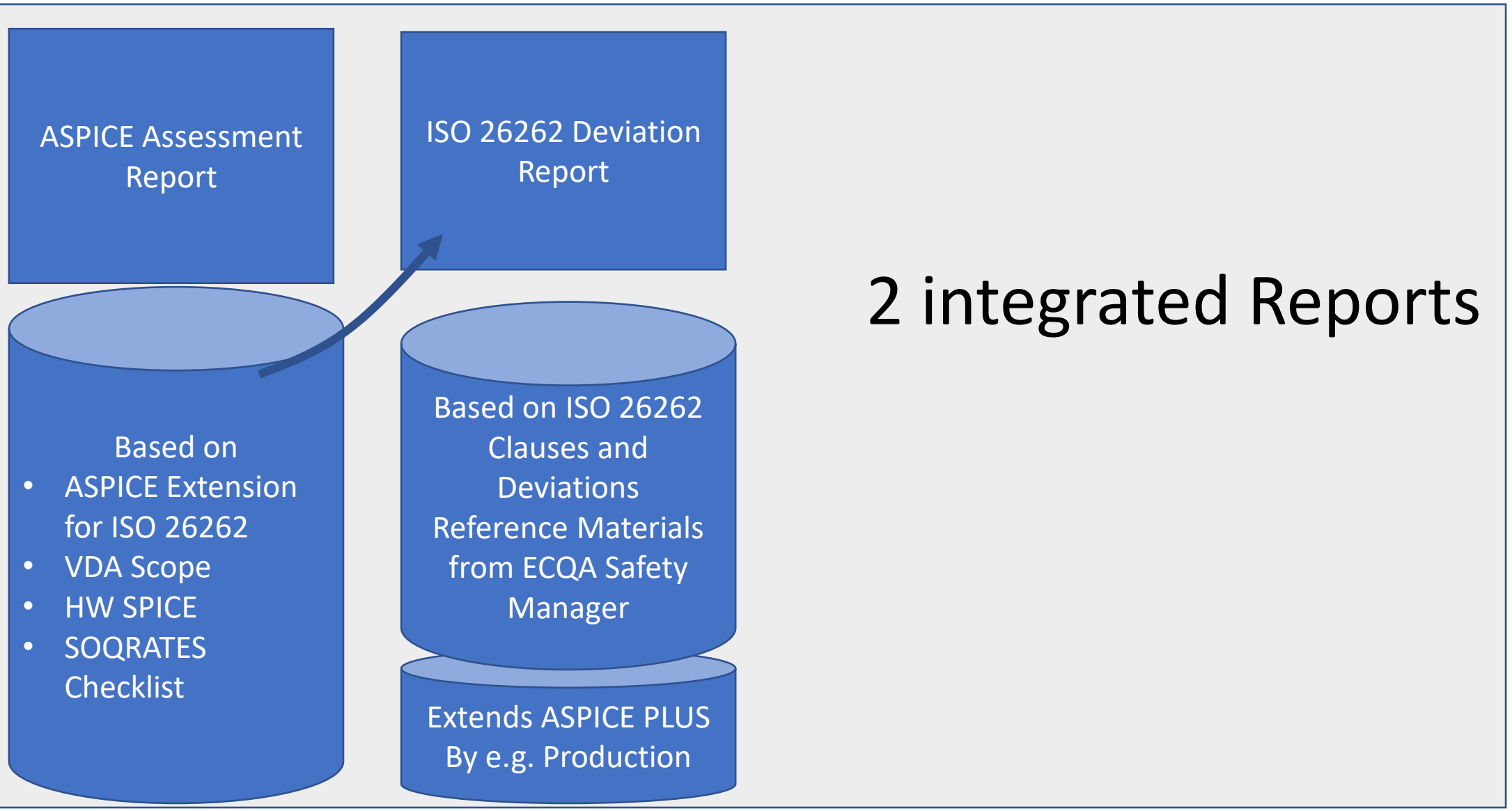
Important Message

Complete Audit after correcting the deviations found in the safety assessment / safety goal checks

Safety Complete Audit

Based on ASPICE+ Extension for VDA Scope +
HW SPICE + Extension from SOQRATES

Sources Used



Reports

- ASPICE assessment report and
- ISO 26262 Deviation Report

Example:

						Legend:		N (Not Adequate)	N	Deviation which cannot be corrected		
								P (Partially Adequate)	P	Deviation which can be corrected with significant effort		
								L (Largely Adequate)	L	Recommendation which can be corrected with little effort		
								F (Fully Adequate)	F	No deviation		
ID	ISO26262 reference					in scope of assessment		FIRMA		Action Plan		
								Evidences Referenced from the Orgamisation	Rating	Improvement Recommendation	Respo	Target
	Part	Clau	Req	Workproduct	Sub-Workproduct		Priority				Who	Date
39	4		5,3	HSI		Yes		The main interfaces are not described in an HSI but are comtaimned in different files. - Interfaces to LED, the current is simaluted based on a datan sheet and temperature profile, and this data is configured as a parameter (in the project this is 780 mA). Parameter name is pLedNomCurrent. - electrical interface of cable connector of CAN. The detail design of the connector is in Visio and the safety assumption is in the safety case. - the file HCM_Parameters_V426_*.xlsm contains a list of all design parameters that can be configured in the software and are dependent on the system layout. - Wire harness: 1060.007.0530_X60_cable_harness_MID_ECE_left.xls	L	Mark these interfaces in the safety case assumptions/descriptions in the safey case v1.9 descriptions. The current system design does not show GND as safety relevant.		

- ✓ Assessments, consulting and training in the field of System, Services and Software Process Improvement and Innovation

- ✓ Organiser of the EuroSPI (European Software, Sytem and Services Process Improvement and Innovation) conference series since 1994 (www.eurospi.net)

- ✓ Founding member, vice-president and technology provider for the European Certification and Qualification Association

- ✓ Accreditated iNTACS™ training provider for Automotive SPICE®

- ✓ Moderator of the German SOQRATES initiative, where 23 leading Germany companies share knowledge concerning process improvement in the field of Functional Safety, Cybersecurity, Traceability…