Experiences with integrated ASPICE and ISO 26262 Assessments

EuroSPI Tech Day, 29.8.2022

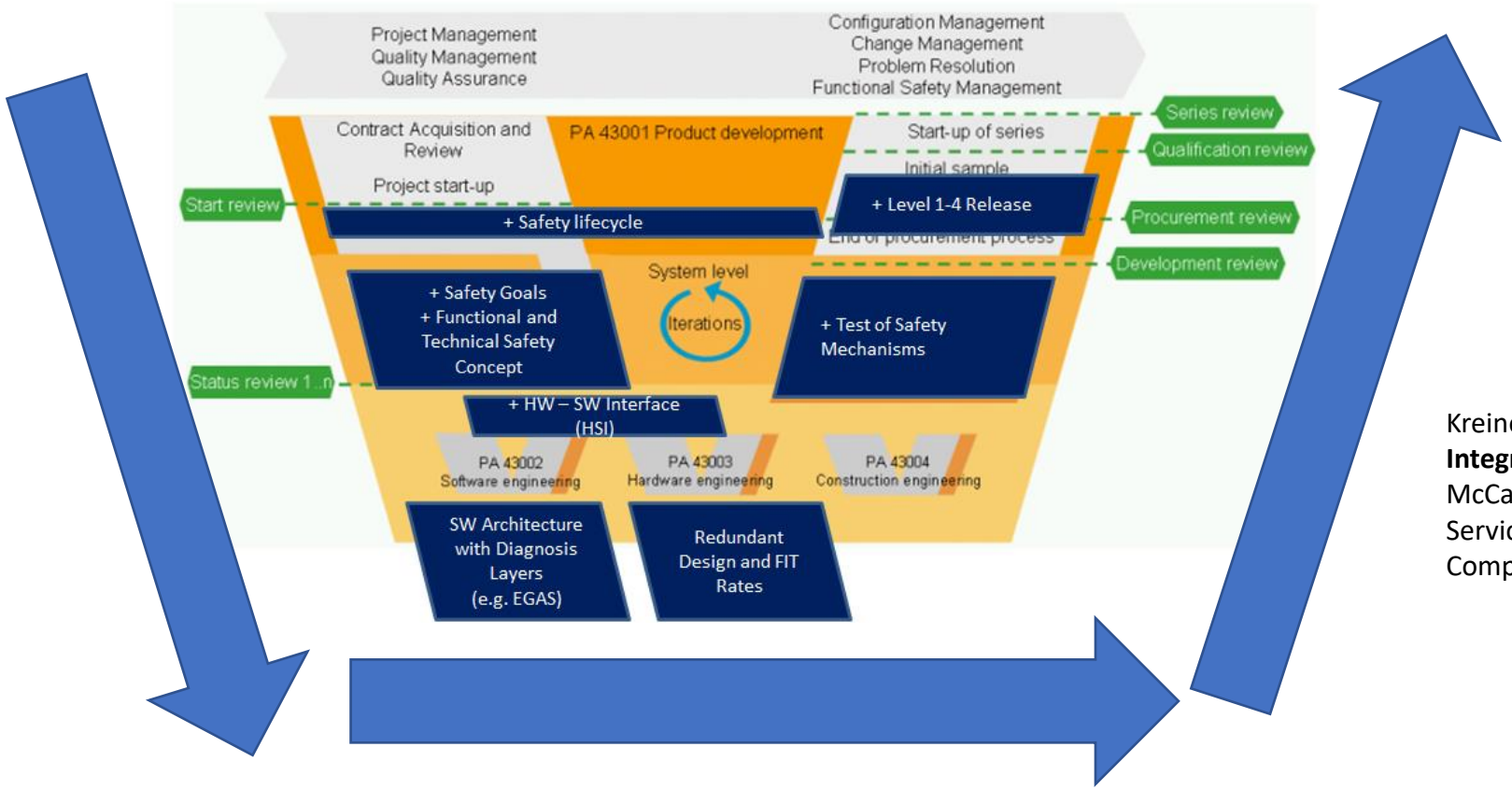
Supported by By SOQRATES Group https://soqrates.eurospi.net

We make your practical safety concept work

Presenter Researcher Profile

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

Motivation – Integrated V-Model



- ✓ 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

- Added safety related work products along the V
- Safety Audit integrating ISO 26262 and ASPICE

Traceability – Integrated V-Model – Extended Questions

ISCN
www.iscn.com

SOQRATES (https://soqrates.eurospi.net , working group)

- Best practices exchange of implementation on a method basis
- Extended safety questions for ASPICE VDA Scope (mainly parts 2,3,4,5,6 of ISO 26262)

Capability Adviser

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

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.1 1
  » SWE.1 2
  » SWE.1 3
  » SWE.1 4
  » SWE.1 5
+ 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.4 System Integration and Integration Test
+ SYS.5 System Qualification Test

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

Software Requirements Analysis — **The purpose of the Software Requirements Analysis Process is to transform the software related parts of the system requirements into a set of software requirements.**

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

☐ **SWE.1.BP1** **Specify software requirements.** Use the system requirements and the system architecture and changes to system requirements and architecture to identify the required functions and capabilities of the software. Specify functional and non-functional software requirements in a software requirements specification. [OUTCOME 1, 5, 7]

ISO 26262 Extended Questions:
- Are software safety requirements in line with the technical safety requirements (Requirements, interfaces, constraints, ?)?
- Are all software safety requirements marked as safety requirements and referred to their source?
- Are semiformal notations used for ASIL C and D?
- Are software safety diagnose requirements assigned to an appropriate diagnose level (e.g. e-gas model with (Level 1 - base diagnosis, Level 2 - independent plausibility checks and functional diagnosis, Level 3 - system control, checking the call sequences, processor, etc.).
- Is the software state machine described and is the safe state clearly separated?
- Is the independence of the monitoring software clearly described?
- Are the software signals specified in the hardware software interface?
- Is there a diagnose matrix describing safety diagnose L2 and L3 functions and the expected fault reaction?
- Are there non functional software requirements relating to the ISO 26262 method tables?
- Are there non functional software requirements relating to the ASIL level assigned influencing the software architecture?
- Is the operating software and the related task management and synchronization of the control software considered?
- Are the appropriate methods used for analysis (see method tables in ISO 26262)?

Safety Assessment – Work Product Reviews – Content Ex 1/2

ISCN
www.iscn.com

SOQRATES (https://soqrates.eurospi.net , working group)

- Best practices review checklists e.g. SEooC Check extract

ID	Crtieria
	State of the Art from SEooC Experience in ASIL D Projects
EXPERIENCE.1	Scope of the SEooC defined?, including processes covered and which not.
EXPERIENCE.2	Assumption of Safety Goals described?
EXPERIENCE.3	ASIL clearly assigned to each safety goal?
EXPERIENCE.4	Assumed FTTI per safety goal is defined?
EXPERIENCE.5	Safety goals are state of the art? (compared to market)
EXPERIENCE.6	Condition of use described (configration, required settings with non tailorable options, expected diagnose on higher layer, quality of inputs like expected input ASIL, etc.)
EXPERIENCE.7	Operating Precautions
EXPERIENCE.8	Integration Precautions
EXPERIENCE.9	HW platforms
EXPERIENCE.10	Architecural overview of components and sub-components available with ASIL decomposition assigned?
EXPERIENCE.11	List of components with a description of their functional meaning.
EXPERIENCE.12	List of interfaces / safety critical SW variables/ date with ASIL assigned (sender/receiver concept)
EXPERIENCE.13	List of function interfaces with ASIL assigned (server/client concept)
EXPERIENCE.14	Safety Critical Function Flow
EXPERIENCE.15	Assumed memory and CPU usage b ythe SEooC?
EXPERIENCE.16	Task / scheduler concept/cycle times/interrupts
EXPERIENCE.17	List of SEooC diagnosis functions/ safety measures which are provided as a service?

Example SEooC Confirmation Review:

More than 50 review criteria for an SEooC in practice

	ISO 26262:2018 Part 10, Clause 9 Criteria
NORM.1	Safety requiremeentsallocated to elemnts in the SEooC
NORM.2	Assumptions defined (on system, software, and hardware level)
NORM.3	ASIL assigned
NORM.4	intended functionality and use context described
NORM.5	Safety requirements assigned to design
NORM.6	Verification activities defined at all levels
NORM.7	Tailoring of the norm for system development (link model for SEooC)
NORM.8	Integration requirements
	ISO 26262:2018 Part 6, Software Safety Analysis
NORM.9	Was the SW safety analysis pattern used , ISO 26262:2018 Figure E.4 Part 6
NORM.10	Agreement of responsibility in case of application project using the SEooC , ISO 26262:2018 Figure E.4 Part 6 (interface clera for new requirements, probelms, test etc.)

Safety Assessment – Work Product Reviews – Content Ex 2/2

ISCN
www.iscn.com

SOQRATES (https://soqrates.eurospi.net , working group)

- Practice versus norm (extended view)

Table 1 — Required confirmation measures, including the required level of independence

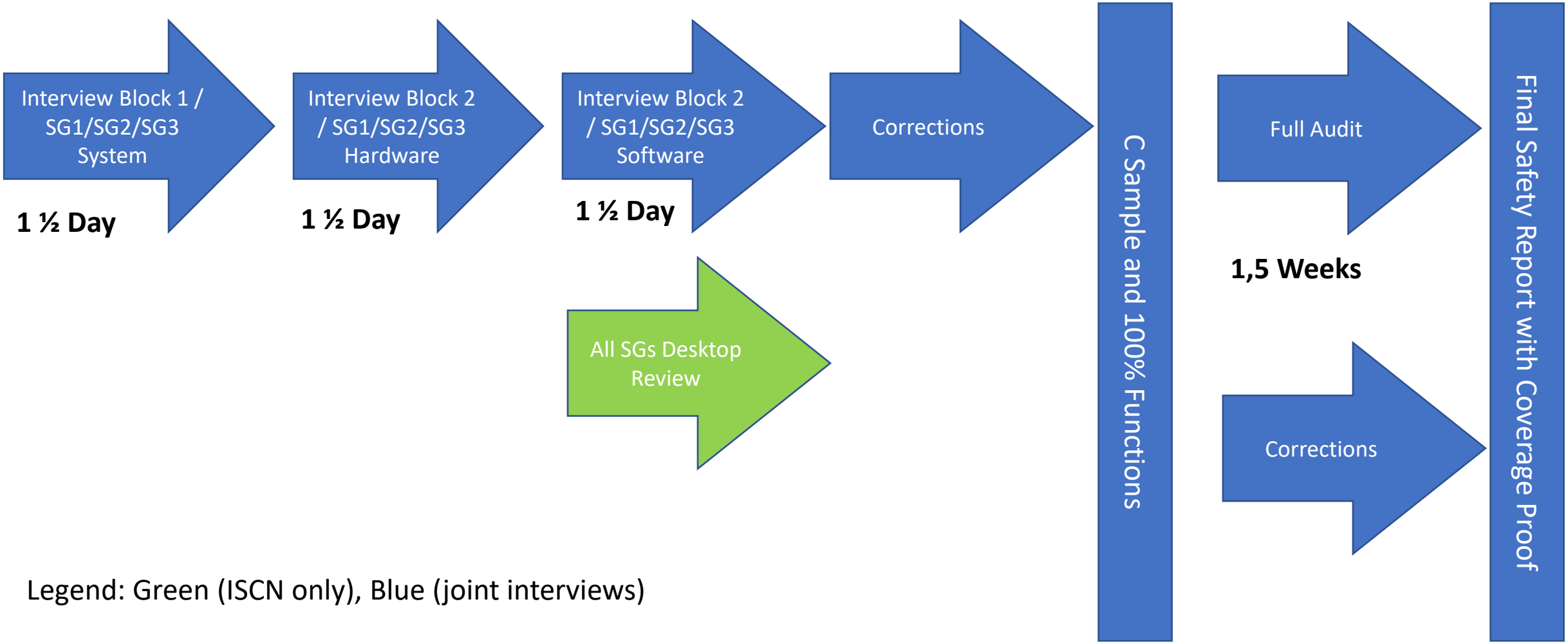
Confirmation measures	Level of independence[a] applies to					Scope
	QM	ASIL A	ASIL B	ASIL C	ASIL D	
Confirmation review of the impact analysis at the item level (see 6.5.1) Independence with regard to the author of the impact analysis and project management	I3	I3	I3	I3	I3	Judgement of whether the impact analysis in accordance with 6.4.3 correctly identified the item as being a new item, a modification of an existing item or an existing item with a modified environment. Judgement of whether the impact analysis in accordance with 6.4.3 adequately identified the implications on functional safety caused by the modification(s); and the safety activities to be performed.
Confirmation review of the hazard analysis and risk assessment (see ISO 26262-3:2018, Clause 6) Independence with regard to the developers of the item, project management and the authors of the work product	I3	I3	I3	I3	I3	Judgement of whether the selection of the operational situations pertinent to the hazardous events and the definitions of the hazardous events are appropriate

Table 1 Part 2 ISO 26262 contains the mandatory confirmation reviews. For all we have expert checklists.

Note: It has e.g. no SEooC Checklist.

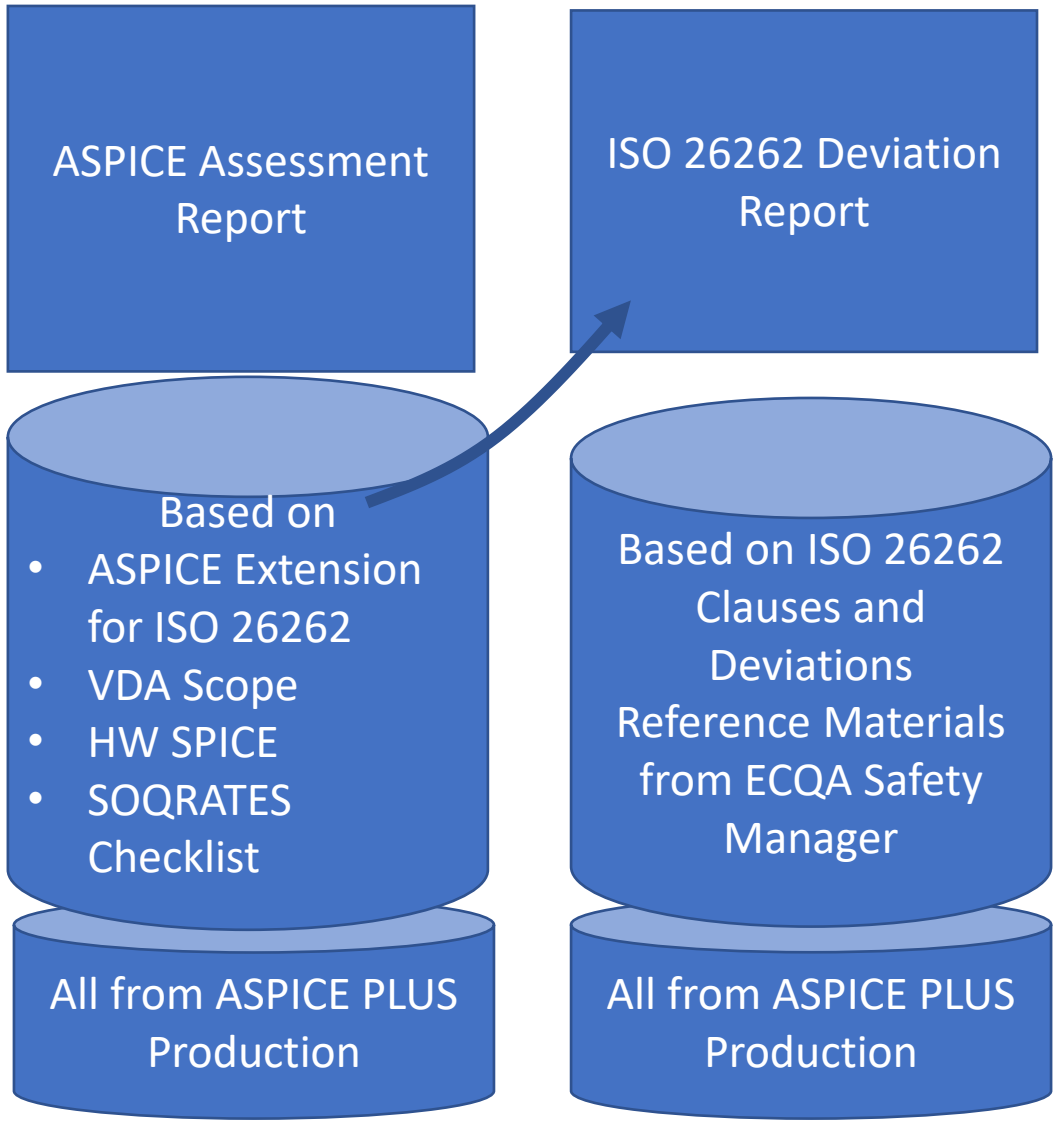
Audit and Assessment Process Flow

ISCN
www.iscn.com



Legend: Green (ISCN only), Blue (joint interviews)

Audit and Assessment Process Flow



2 integrated Reports

Audit and Assessment Process Flow

ISCN
www.iscn.com

ASPICE Capability Levels and Profile

ASPICE Assessment Report (with extended questions)

Plus ISO 26262 clause rating and deviation report

						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.		

Thanks

Thank you for cooperating with ISCN.

1. ISCN is INTACS certified training provider for Automotive SPICE assessor courses
2. ISCN is certified by VDA to hold provisional and competent ASPICE assessor courses

3. ISCN moderates the German task force SOQRATES (https://soqrates.eurospi.net) since 2003 where >20 Tier 1 collaborate on ASPICE, Safety and Security.

4. ISCN organises the EuroSPI conference since 1994 where e.g. VW is organising a workshop community, and VW, Rheinmetall AG, EB, MAGNA, AVL held key notes. http://www.eurospi.net

5. EuroSPI certificates are issued by EuroSPI Certificates & Services GmbH (www.eurospi.net) in cooperation with DRIVES and the Automotive Skills Alliance (ASA). The ASA was founded by the EU Blueprint Project Drives and ALBATTS with support from the European Automobile Manufacturers' Association (ACEA). https://www.eurospi.net. ISCN is founding member.

Thanks

ISCN
www.iscn.com

Thank you for cooperating with EuroSPI Certificates GmbH.

1. Academy – Courses and Training Platform
2. Certification – Exam system and cerrificates
3. EuroSPI Conference Series
4. Assessment Tool – ISO 330xx based