

Experiences with ASPICE for Cybersecurity Assessments

EuroSPI Tech Day, 28.8.2023

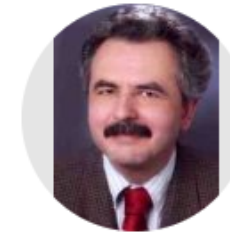
Supported by By SOQRATES Group <https://soqrates.eurospi.net>

Dr Richard Messnarz

- PhD in Technical Mathematics and Informatics from TU Graz
- **Instructor Competent Level Automotive SPICE** Trainer/ Assessor
- INTACS VDA Certified **Trainer ASPICE for Cybersecurity (member of development team)**
- **VW-SQIL**
- 34 years Automotive experience
- EuroSPI/ASA (Automotive Skills Alliance) **Certified Cybersecurity Engineer/Manager Trainer**
- EuroSPI/ASA (Automotive Skills Alliance) **Certified Functional Safety Manager and Trainer**
- **ISO 26262 ASIL B, ASIL C and ASIL D project experiences** (also as Safety Manager, Safety Engineer or Assessor)
- **Experiences with cybersecurity ASPICE assessments** and cybersecurity projects / implementations
- Chair and founder of EuroSPI conferenceseries <https://conference.eurospi.net/index.php/en/>
- Editor of EuroSPI book series <https://link.springer.com/conference/eurospi>
- Moderator of SOQRATES working group of Tier 1 and OEMs – Experience exchange in ISO 26262, ISO 21434, ASPICE, and HAD vehicle topics

Research Profile

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



Richard Messnarz

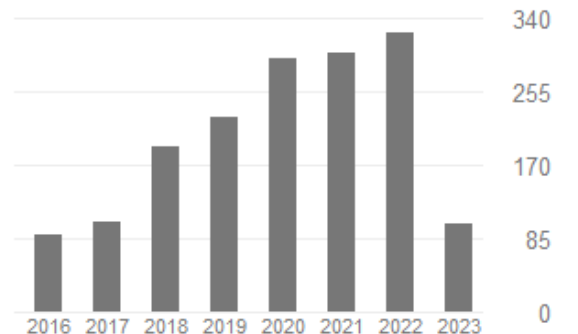
ISCN GesmbH

Bestätigte E-Mail-Adresse bei iscn.com - [Startseite](#)

[SPI Functional Safety Autom...](#)

Zitiert von [ALLE ANZEIGEN](#)

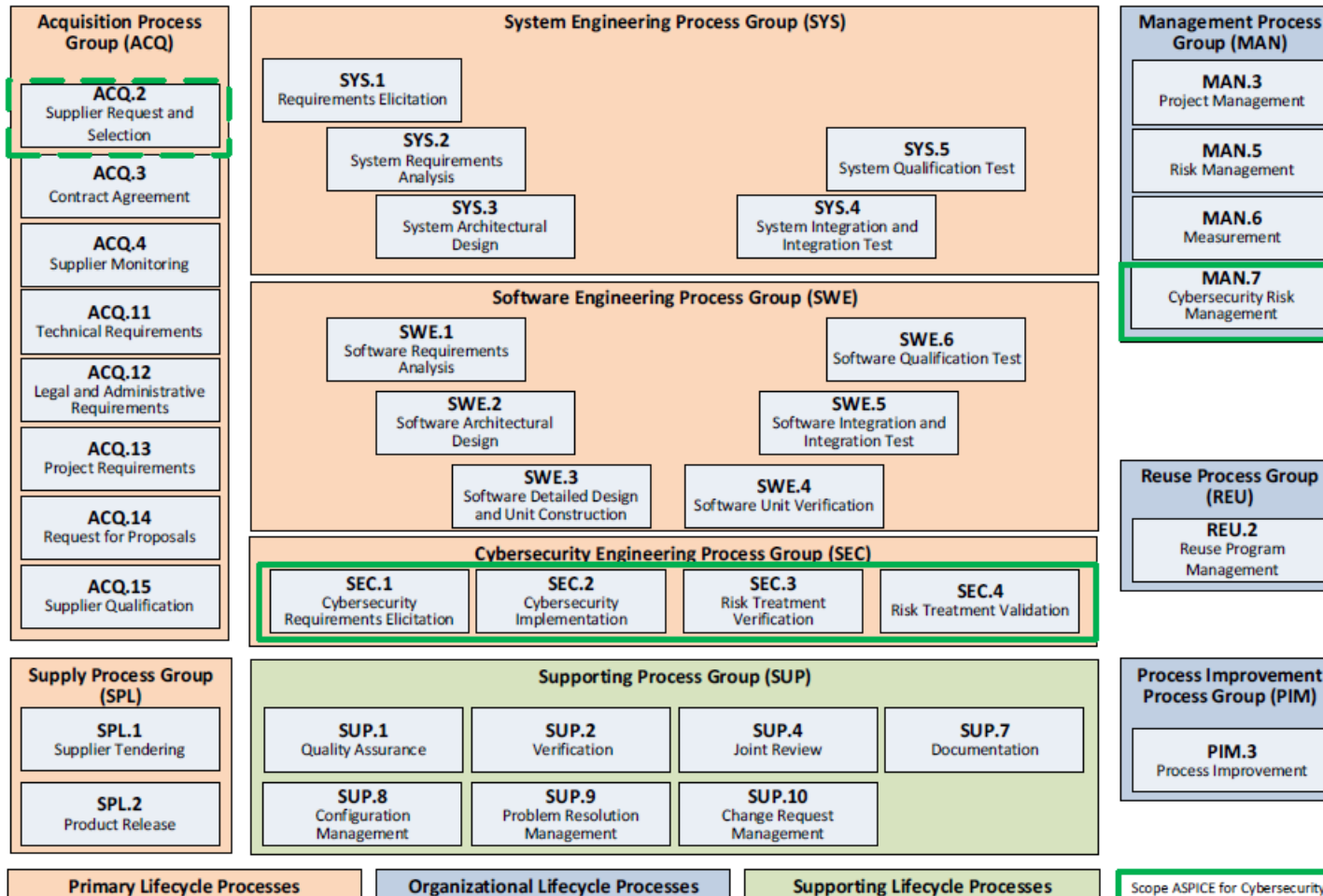
	Alle	Seit 2018
Zitate	2527	1440
h-index	27	17
i10-index	82	49



5 Important Practical Experiences Shared at TechDay

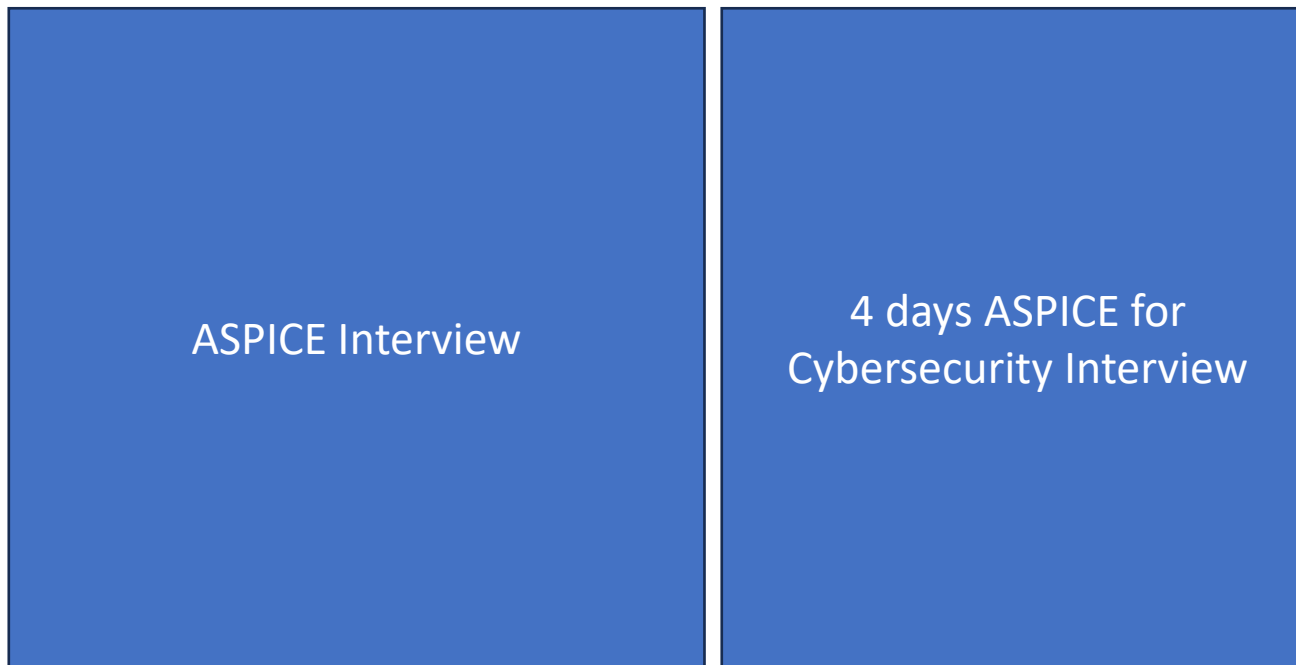
Attend the key note at the EuroSPI Conference for more

- ISCN Experiences with the assessment model (in assessments with co-assessors from AUDI AG, MB, lead Tier 1).

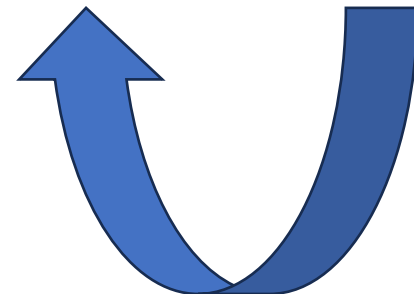


- MAN.7, SEC.1, SEC.2, SEC.3 have always been selected for the assessments.
- ACQ.2 so far has not been selected at all
- ACQ.4 (not marked in model, only in guideline mentioned as extended) was always selected and had to be rated separately for the CS relevant supplier
- SEC.4 penetration test had to be done by an independent organisation. Still SEC.4 at Tier has been assessed for the cybersecurity case validation part. And the contract and reports from the penetration test were checked.

- ISCN Experiences with the interview plan and consolidation of overall results



- In AUDI/VW case the ASPICE for cybersecurity interview was done after the ASPICE interviews.
 - Attention: If rating in SEC.x processes was then low, this had an impact on the overall rating also of SYS.x and SWE.x
- In MB case the assessments we had did not make an extra interview, we checked the TARA, SSA of MB, NEST Test etc. and we rated normal ASPICE processes down in case of missing cybersecurity practices.
 - Attention: They told us that they consider also the ASPICE for Cybersec ratings in future.



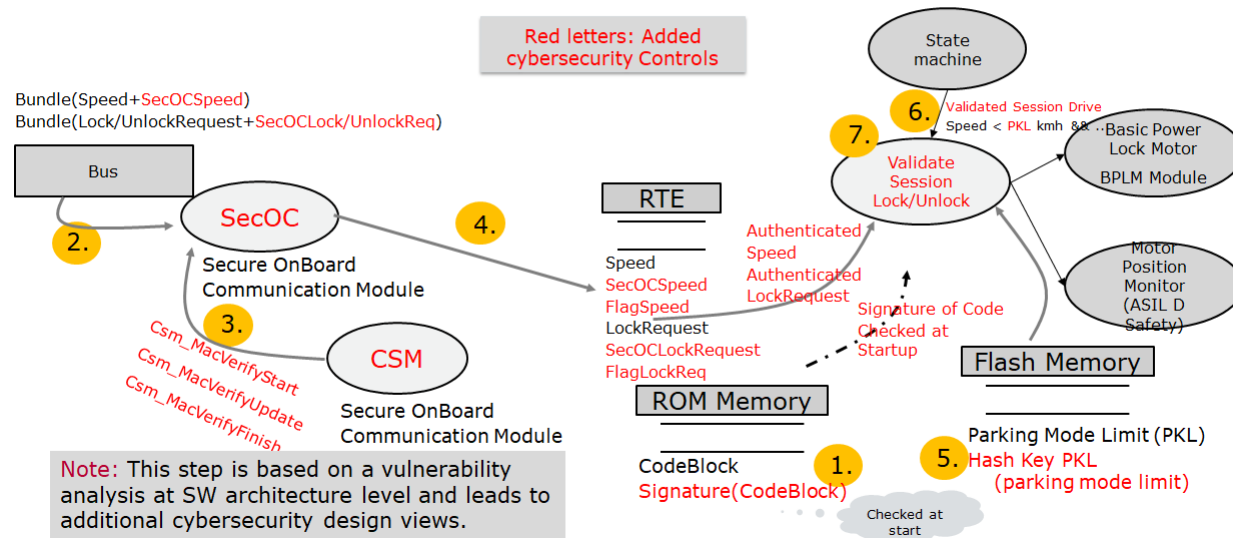
[SEC.1.RL.2] If BP6 for MAN.7 is downrated, this shall be in line with the rating of the indicator BP1.

[SEC.1.RC.3] If BP1 for SYS.2 is downrated, this should be in line with the rating of the indicator BP1.

[SEC.1.RC.4] If BP1 for SWE.1 is downrated, this should be in line with the rating of the indicator BP1.

- ISCN Experiences with understanding the practices in the ASPICE for Cybersecurity model

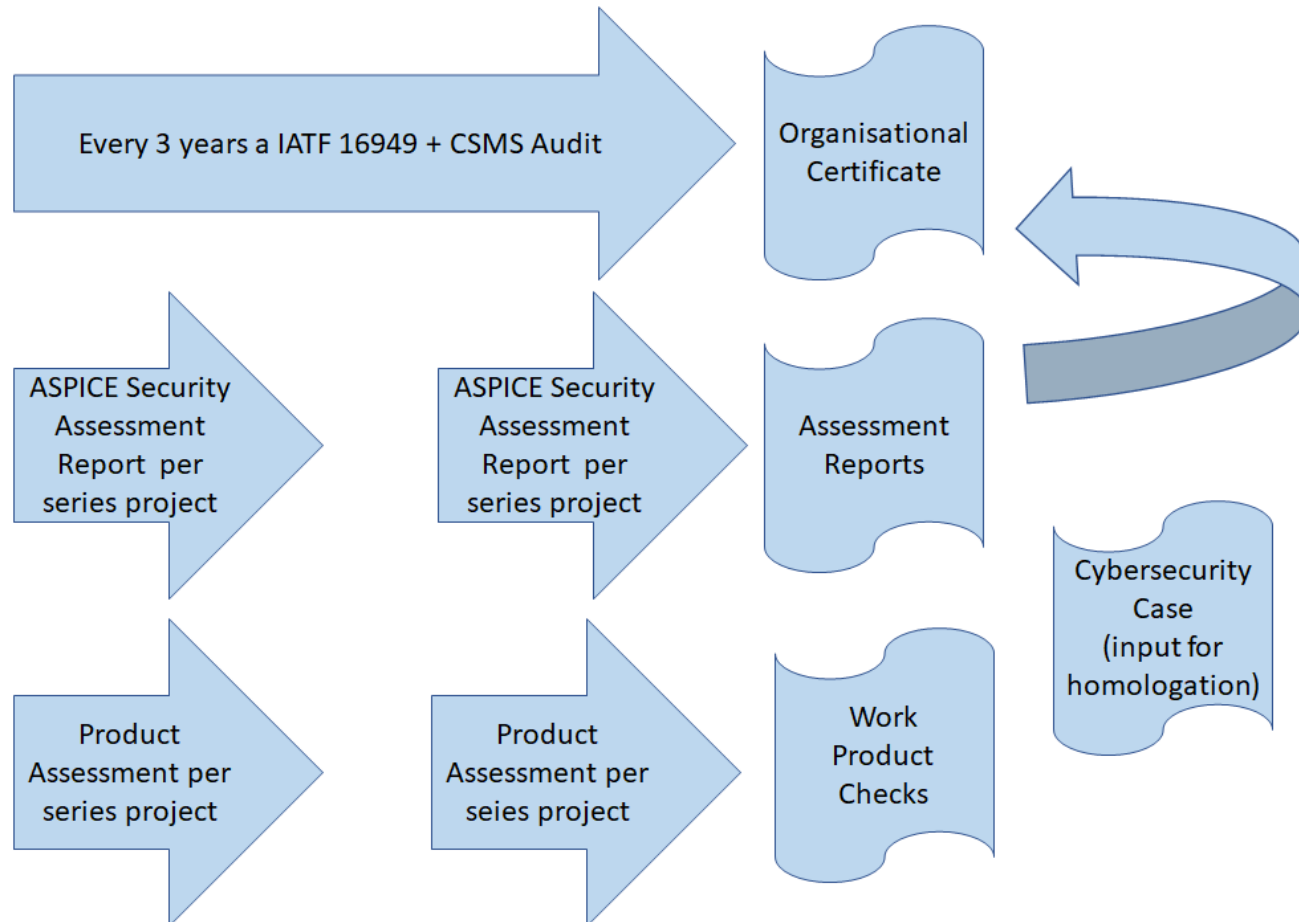
Simplified functional flow after adding the cybersecurity controls



- The **code block** of the SW in the ROM is **signed** with a key (no authenticated code change has happened).
- Authentication** and integrity of the messages lock/unlock request, speed by SecOC (Secure OnBoard Communication) and MAC (Message Authentication Code).
- The lib SecOC uses the CSM lib **MacVerify function** to check the message **authenticity**.
- On RTE if **MacVerify** is failing a fault flag is set.
- The speed parameter is secured by a **hash key (data integrity)**.
- , (7) Before a lock/unlock command is further interpreted (for whitelisting strategy of functions) a **validation session** drive mode function checks the state of the system (**speed authentication** was ok, lock/unlock request **message authentication** is ok, etc.) and then calls the Basic Power Lock Motor function of the electronic motor control unit.

- The ASPICE for Cybersecurity Assessment Model is not enough to understand what exactly an assessor needs to check.
- The ASPICE for Cybersecurity Guideline provides more details, still misses practical examples of work products an assessor needs to find.
- Therefore IT IS REQUIRED to look in detail at the INTACS training materials and examples. E.g. Do you know how a modelled cybersecurity use case should look like? Or, e.g. Do you know the functions an HSM normally would offer, do you ask this in the assessment scope?
- And you need to be interested to read and learn from examples.

- ISCN Experiences with relationships between TISAX, CSMS Audit and ASPICE for Cybersecurity



- A lot of misunderstanding at top management still:
 - The manager stated (not saying which Tier 1): “We have the TISAX successfully passed, so he expects a level 1 Fully now in all ASPICE for Cybersecurity Processes!”.
- In reality you can still have level 0 in all ASPICE for cybersecurity processes, even if TISAX is in place!

- ISCN Experiences with assessment performance

Capability Adviser



All Assessments Evidences Export Rating Settings Raspberry Help Logout

All Units

- + MAN.3 Project Management
- + MAN.7 Cybersecurity Risk Management
- SEC.1 Cybersecurity Requirements Elicitation
 - » SEC.1.1
 - » SEC.1.2
 - » SEC.1.3
 - » SEC.1.4
 - » SEC.1.5
- + SEC.2 Cybersecurity Implementation
- + SEC.3 Risk Treatment Verification
- + SEC.4 Risk Treatment Validation
- + 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.1 Requirements Elicitation
- + SYS.2 System Requirements Analysis
- + SYS.3 System Architectural Design
- + SYS.4 System Integration and Integration Test
- + SYS.5 System Qualification Test

VDA Scope + Cybersecurity
+ SYS.1 - ACQ.2 - ACQ.4

Cybersecurity Requirements Elicitation The purpose of the Cybersecurity Requirements Elicitation Process is to derive cybersecurity goals and requirements from the outcomes of risk management, and ensure consistency between the risk assessment, cybersecurity goals and cybersecurity requirements.

SEC.1.1: Summary Notes Save All Evidences Recommendations Rules

SEC.1.BP1 **Derive cybersecurity goals and cybersecurity requirements.** Derive cybersecurity goals for those threat scenarios, where the risk treatment decision requires risk reduction. Specify functional and non-functional cybersecurity requirements for the cybersecurity goals, including criteria for the achievement of the cybersecurity goals. [OUTCOME 1, 2]

Cybersecurity requirements may address, among others:

- Functions that are implemented in mechanics, hardware or software, or cover a combination of these elements
- Processing of signals from other systems
- Non-functional requirements

Unclear or generic requirements have to be clarified with the individual stakeholders.
Non-functional requirements at a system level may be decomposed into functional requirements on a component level - for example, when cybersecurity of a system is a non-functional requirement. This non-functional requirement may be detailed into functional requirements for hardware and software components.

[SEC.1.RC.1] If unclear or inconsistent requirements are not clarified with the individual stakeholders, indicator BP1 should be downrated.
[SEC.1.RC.2] If the cybersecurity requirements specification does not reflect the results of the risk assessment, BP1 should not be rated higher than L.

N P L F Not App. Note

- Assessments for systems that integrate cybersecurity stacks and further function libs are usually with distributed teams.
- This then requires an infrastructure where in a hybrid set up teams assessors are onsite and online and work through an assessment tool / infrastructure.
- The tool must support teamwork and the guidelines.

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 ALBATTIS with support from the European Automobile Manufacturers' Association (ACEA). <https://www.eurospi.net>. ISCN is founding member.

Thanks

Thank you for cooperating with EuroSPI Certificates GmbH.



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