

# Experiences with CSMS Audit preparation using the Capability Adviser supported CSMS process assessment model

**EuroSPI Tech Day, 2.9.2024**

Bernhardt Steger, ISCN Group, Austria,  
Dr Richard Messnarz, ISCN & EuroSPI GmbH,  
Damjan Ekert, ISCN & EuroSPI GmbH

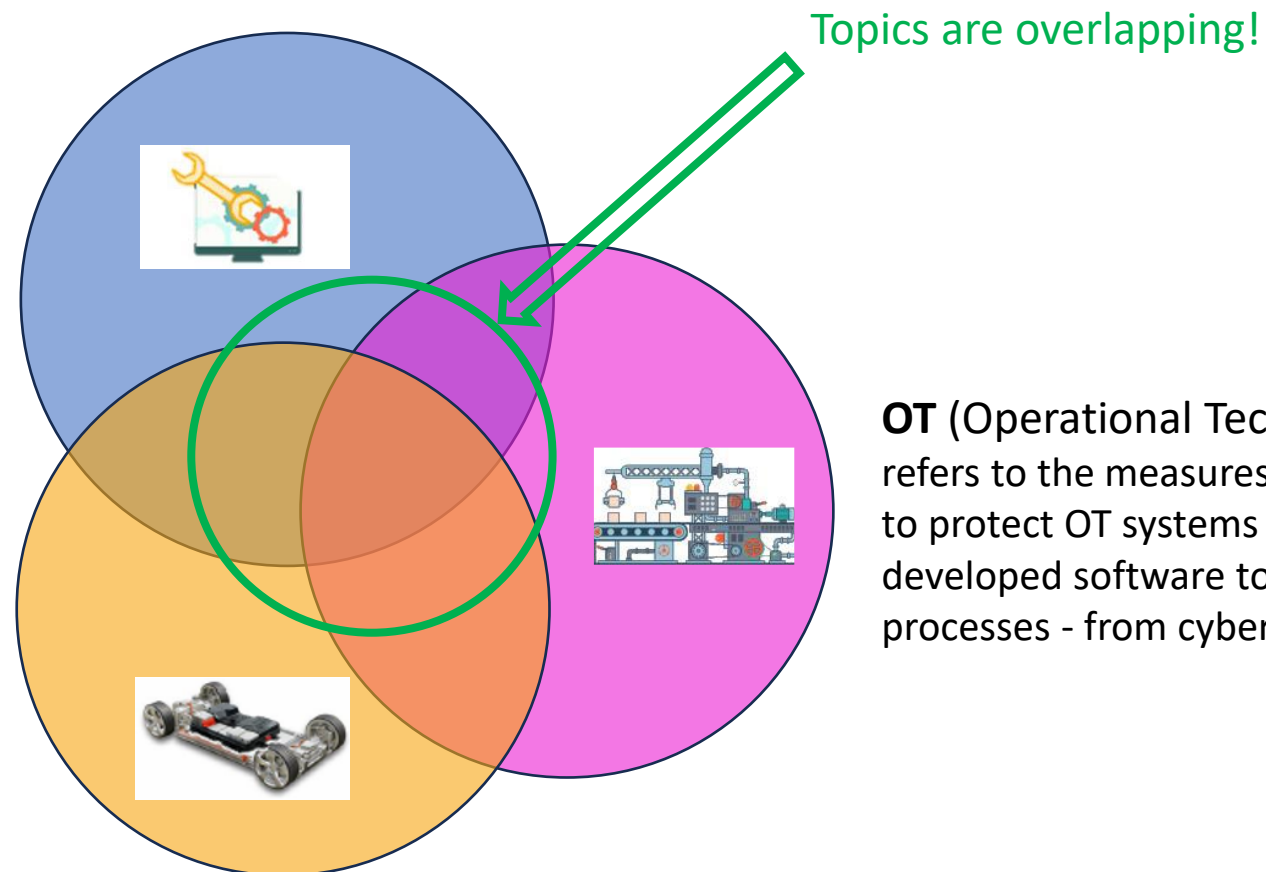
# (Cyber)Security – (Simplified) Overview

## IT (Information Technology) Security

is the protection of computer software, systems and networks from threats that may result in unauthorized information disclosure, theft of (or damage to) hardware, software, or data, as well as from the disruption or misdirection of the services they provide.

## Product Security

includes the policies, processes and practices used to protect a product's software, hardware and digital services from malicious attacks, data breaches and other security risks.



## OT (Operational Technology) Security

refers to the measures and controls used to protect OT systems - which use specially developed software to automate industrial processes - from cyber security threats.

# Security and Certificates – (Simplified) Overview

## IT (Information Technology) Security

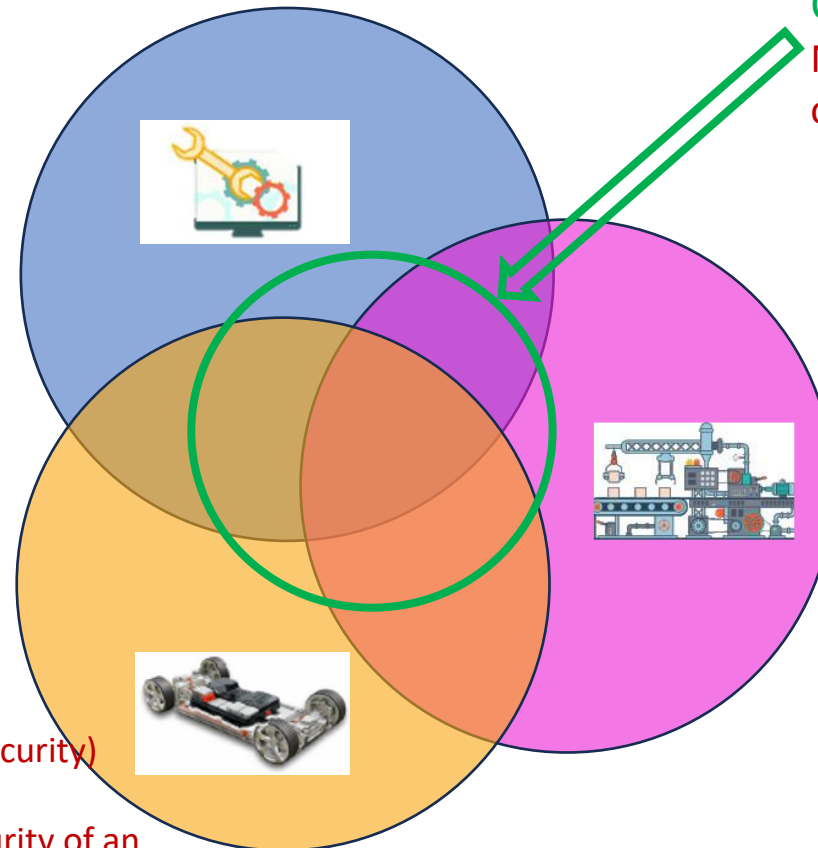


TISAX

## Product Security



Cybersecurity Audit  
(e.g.: Automotive SPICE® for Cybersecurity)  
Cybersecurity Assessment  
(judges independently the cybersecurity of an  
item or component)



Certificates are overlapping!  
No 1:1 connection between type  
of security and certificate!

## OT (Operational Technology) Security



(A)CSMS – (Automotive)  
Cybersecurity Management System  
(Audit) for compliance with UNECE  
R-155, either

- ISO/PAS 5112 / ISO/SAE 21434
- VDA QMC Audit Schema (“VDA Redbook”)

# (Automotive) Cybersecurity Management System

**(A)CSMS** = a systematic, risk-based approach that defines organisational processes, responsibilities and governance structures to address risks associated with cyber threats to vehicles and protect them from cyber attacks. (UNECE R-155)

Therefore, an organization has to provide evidences that:

- The organizational setup ensures that cybersecurity activities can be successfully executed within an organization.
- Processes are established, policies are rolled out, roles and responsibilities are defined, toolchains are in place, trainings are available, people with cybersecurity awareness are assigned to projects, ...

(A)CSMS is typically assessed by an audit (e.g. like ISO 9001). The certificate has to be renewed every three years.

# Comparison of (basis of) (A)CSMS Audits

## ISO/PAS 5112 / ISO/SAE 21434

- Based either on questionnaire of PAS 5112 and/or (directly) on chapter structure of ISO 21434.

1. General considerations	
2.1 Cybersecurity governance	2.2 Cybersecurity leadership
2.3 Cybersecurity strategy	2.4 Cybersecurity objectives
2.5 Cybersecurity risk management	2.6 Cybersecurity metrics
2.7 Cybersecurity performance evaluation	2.8 Cybersecurity improvement
3. Cybersecurity by activities	3.1 Cybersecurity by design
3.2 Cybersecurity by development	3.3 Cybersecurity by testing
3.4 Cybersecurity by operations and maintenance	3.5 Cybersecurity by disposal
3.6 Cybersecurity by support and decommissioning	3.7 Cybersecurity by other activities
4. Cybersecurity by products	4.1 Cybersecurity by product development
4.2 Cybersecurity by product testing	4.3 Cybersecurity by product operations and maintenance
4.4 Cybersecurity by product disposal	4.5 Cybersecurity by product support and decommissioning
5. Cybersecurity by processes	5.1 Cybersecurity by process development
5.2 Cybersecurity by process testing	5.3 Cybersecurity by process operations and maintenance
5.4 Cybersecurity by process disposal	5.5 Cybersecurity by process support and decommissioning
6. Cybersecurity by people	6.1 Cybersecurity by personnel selection
6.2 Cybersecurity by personnel training	6.3 Cybersecurity by personnel awareness
6.4 Cybersecurity by personnel performance	6.5 Cybersecurity by personnel retention
6.6 Cybersecurity by personnel exit	6.7 Cybersecurity by personnel support and decommissioning
7. Cybersecurity by information and communication	7.1 Cybersecurity by information management
7.2 Cybersecurity by communication management	7.3 Cybersecurity by information security
7.4 Cybersecurity by communication support and decommissioning	7.5 Cybersecurity by information security support and decommissioning
8. Cybersecurity by technology	8.1 Cybersecurity by technology selection
8.2 Cybersecurity by technology testing	8.3 Cybersecurity by technology operations and maintenance
8.4 Cybersecurity by technology disposal	8.5 Cybersecurity by technology support and decommissioning
9. Cybersecurity by other activities	9.1 Cybersecurity by other activities selection
9.2 Cybersecurity by other activities testing	9.3 Cybersecurity by other activities operations and maintenance
9.4 Cybersecurity by other activities disposal	9.5 Cybersecurity by other activities support and decommissioning



- During audit, usually each requirement is explicitly checked (or Q1 – Q6).
- (Usually used) rating (for each question): **D**(eviation) – **R**(ecommendation) – **I**(nformation)
- Usually, an extra audit: Stage-1 and Stage-2 audit(s).

## VDA QMC Audit Schema (“VDA Redbook”)



- Catalogue of questions and rating schema for the auditing of OEMs and their subcontractors for information security.
- Questionnaire (Q1 – Q7) covers all CSMS (Cybersecurity Management System) aspects required by the UNECE R-155.
- For each question the auditor estimates the risk.
- (Overall) rating schema: **C B A**.
- Usually, audit is part of IATF 16949 (ISO 9001, ...).

approach chosen by ISCN (using **NPLF**)

# VDA QMC Audit Schema for the implementation of UNECE (A)CSMS

Example audit question:

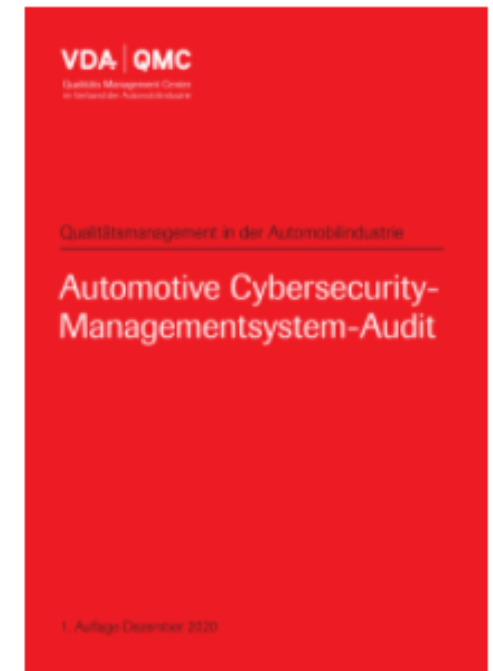
Q5.1 Is a process established to specify cybersecurity requirements?

Relevant minimum requirements

It is organizationally ensured that cybersecurity requirements are specified for the cybersecurity goals, including a rationale for the achievement of these goals.

The cybersecurity requirements are refined based on

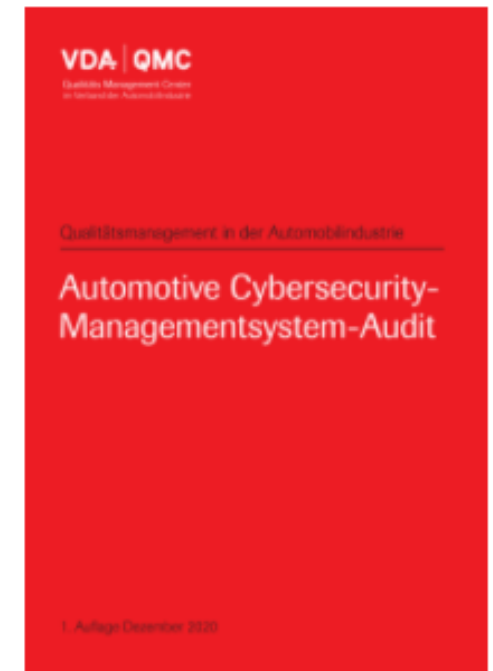
- a) cybersecurity requirements that are allocated from higher level, and
- b) architectural design from higher level



# VDA QMC Audit Schema for the implementation of UNECE (A)CSMS

Example(s) of evidences/indicators for:  
Q5.1 Is a process established to specify cybersecurity requirements?

- Documentation of requirements for the cybersecurity concept.
- Description of the high-level architectural design as a basis for the cybersecurity concept.



# Capability Adviser Configured for (A)CSMS

The screenshot shows the 'Capability Adviser' interface. At the top, there are navigation tabs: 'All Assessments', 'Export', 'Rating', and 'Settings'. Below these are sub-tabs for 'CSMS.1 - Level 1', 'Evidences', 'Consistency', 'Overview', and 'Consolidation'. The main content area is titled 'CSMS Audit' and includes a sidebar with a tree view of units:
 

- CSMS.1 Management
  - » CSMS.1 - Level 1
- + CSMS.2 Risk Identification
- + CSMS.3 Risk Assessment, Categorization and Management
- + CSMS.4 Consistency Check
- + CSMS.5 Specification, Verification, Validation and Release
- + CSMS.6 Updating the Risk Assessments
- + CSMS.7 Incident Response
- + CSMS.8 Reporting against Authorities
- + CSMS.9 Management in the Supply Chain

 The main panel shows the 'Management' section for 'CSMS.1.Q1 Define a cybersecurity policy'. It includes a list of examples for Q1, a rating scale (N, P, L, F, Not App.) with 'L' selected, and text boxes for 'Strengths' and 'Weaknesses'. A blue arrow points to the 'All Units' section in the sidebar.



All (A)CSMS processes

All questions analysed, strengths and weaknesses documented, and rated based on the N/P/L/F scale.



# Experiences with (A)CSMS Audit Preparation

- ✓ Good „compromise“ to provide audit environment (incl. rating) known by both security „worlds“ (TISAX vs ASPICE®).
  - ✓ Strengthens the bi-directional awareness between responsables for IT security (e.g.: CISO) and product development (R&D) (supported by possible discussions of given examples):
    - ✓ Who is expected to provide which evidence?
    - ✓ Supports understanding of needed cooperation between both security „worlds“ (e.g.: tool list, continuous security activities).
    - ✓ Clarifies „changes“ to engineering (life-)cycles of products (so far, R&D support ended soon after SOP, due to security, engineering resources have to be provided at least until end of maintenance phase).
  - ✓ List of open issues (based on found weaknesses resp. final analysis report exported from CapAdv) supports closing the gaps.
- ❗ VDA QMC audit schema is not detailed based on single ISO/IAE 21434 requirements.

# 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](http://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