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

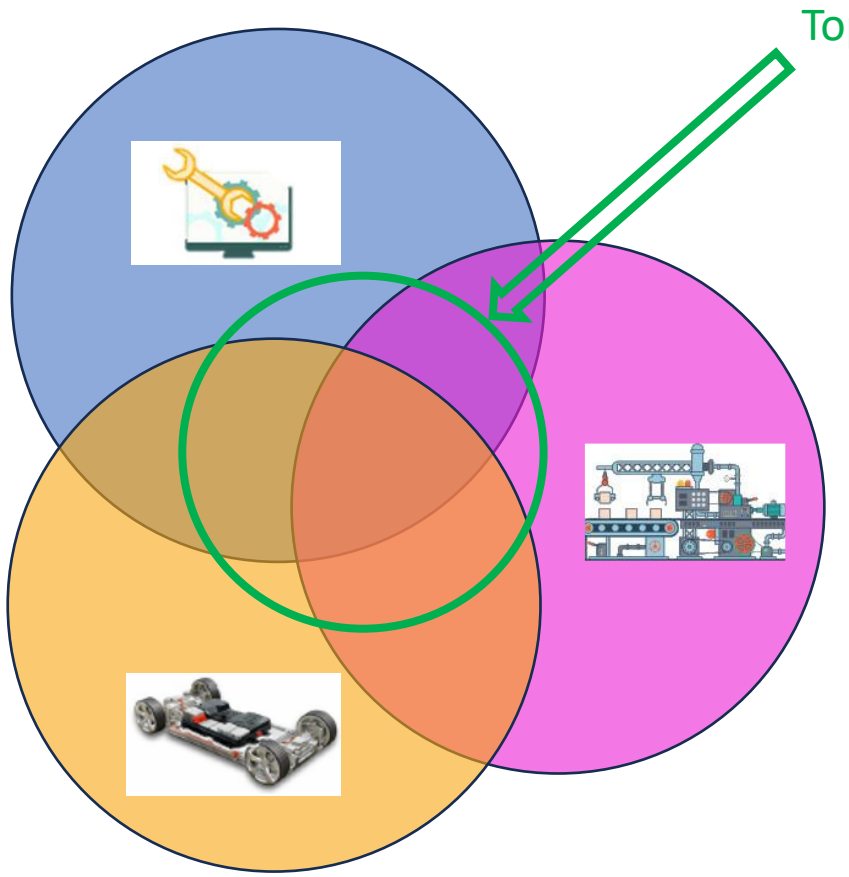
EuroSPI Tech Day, 2.9.2024

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.

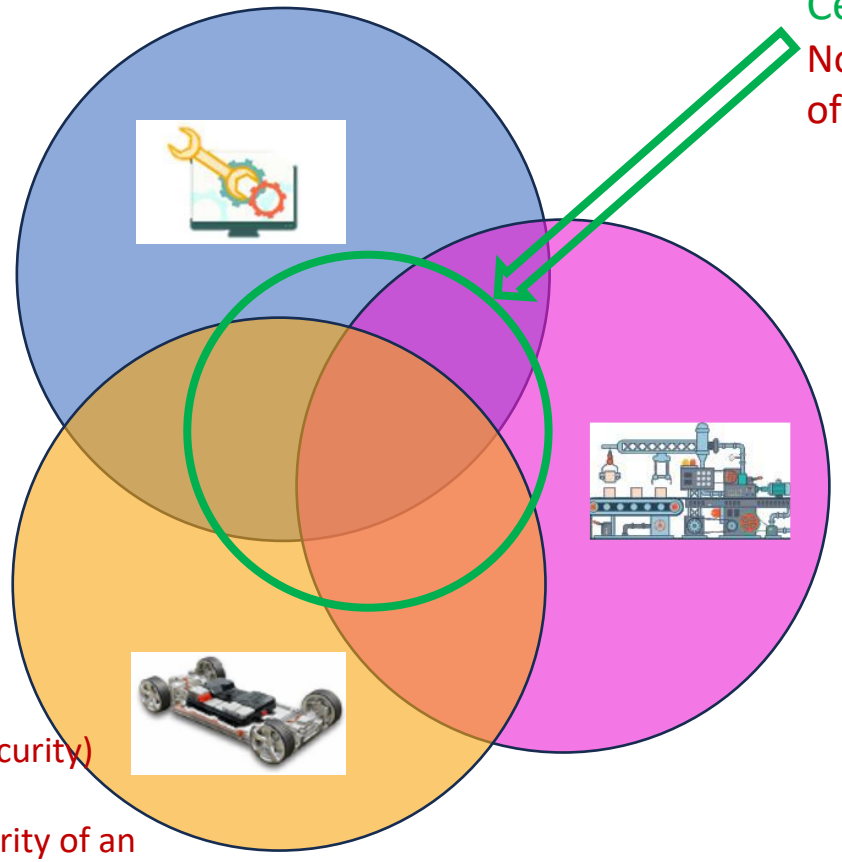


OT (Operational Technology) **Security** refers to the measures and controls used to protect OT systems - which use specially developed software to automate industrial processes - from cyber security threats.

Security and Certificates – (Simplified) Overview

IT (Information Technology) **Security**

TISAX



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”)

Product Security

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

(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:

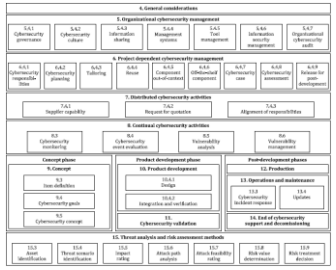
- The organizational setup ensures that cybersecurity activities can be successfully executed within an organization.
- Processes are established, policies are rolled out, roles and responsibilities are defined, toolchains are in place, trainings are available, people with cybersecurity awareness are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



- During audit, usually each requirement is explicitely 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”)

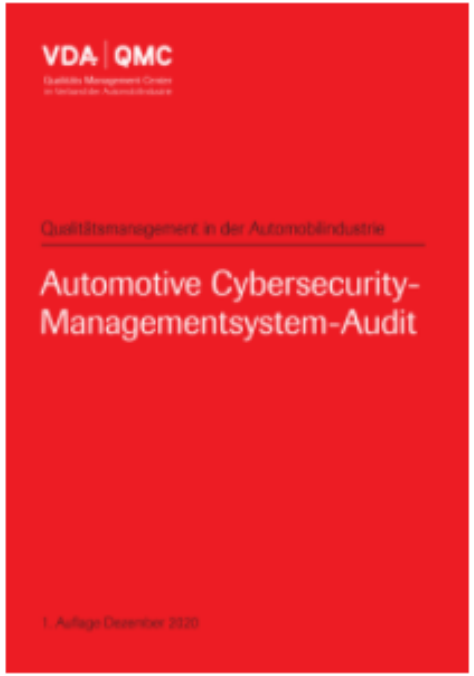
- Catalogue of questions and rating schema for the auditing of OEMs and their subcontractors for information security.
- Questionnaire (Q1 – Q7) covers all CSMS (Cybersecurity Management System) aspects required by the UNECE R-155.
- For each question the auditor estimates the risk.
- (Overall) rating 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

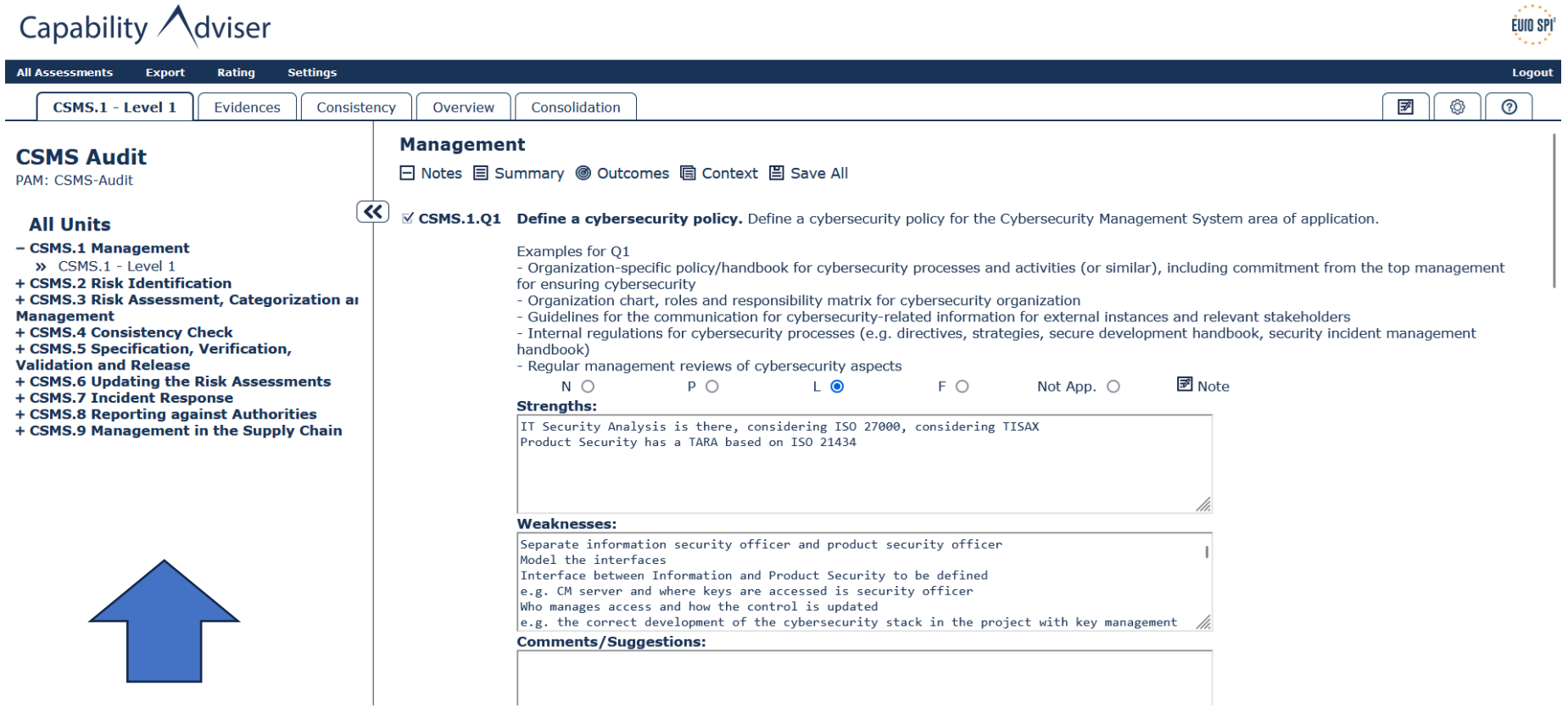
VDA QMC Audit Schema for the implementation of UNECE (A)CSMS

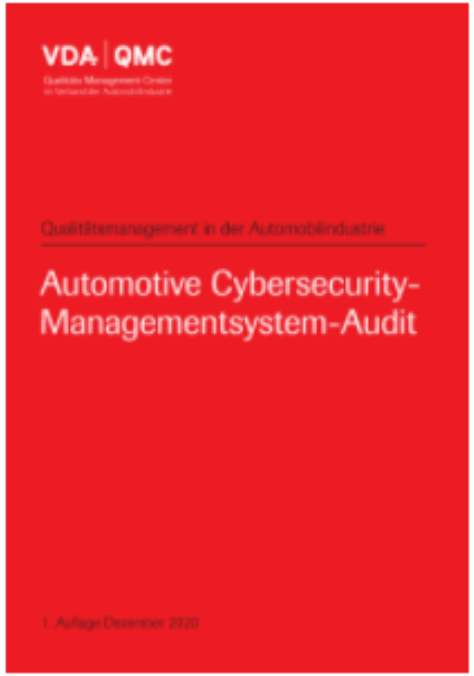
Example(s) of evidences/indicators for:

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





All (A)CSMS processes

All questions analysed, strengths and weaknesses documented, and rated based o 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 responsibles 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) 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