AUTOMOTIVE SPIN ITALIA

Automotive Cybersecurity – Different Aspects

Hidden Object | Oggetto Nascosto

2021-May-27
Thomas Liedtke (PhD)

KUGLER MAAG CIE
besser mit uns

Thomas Liedtke (PhD)

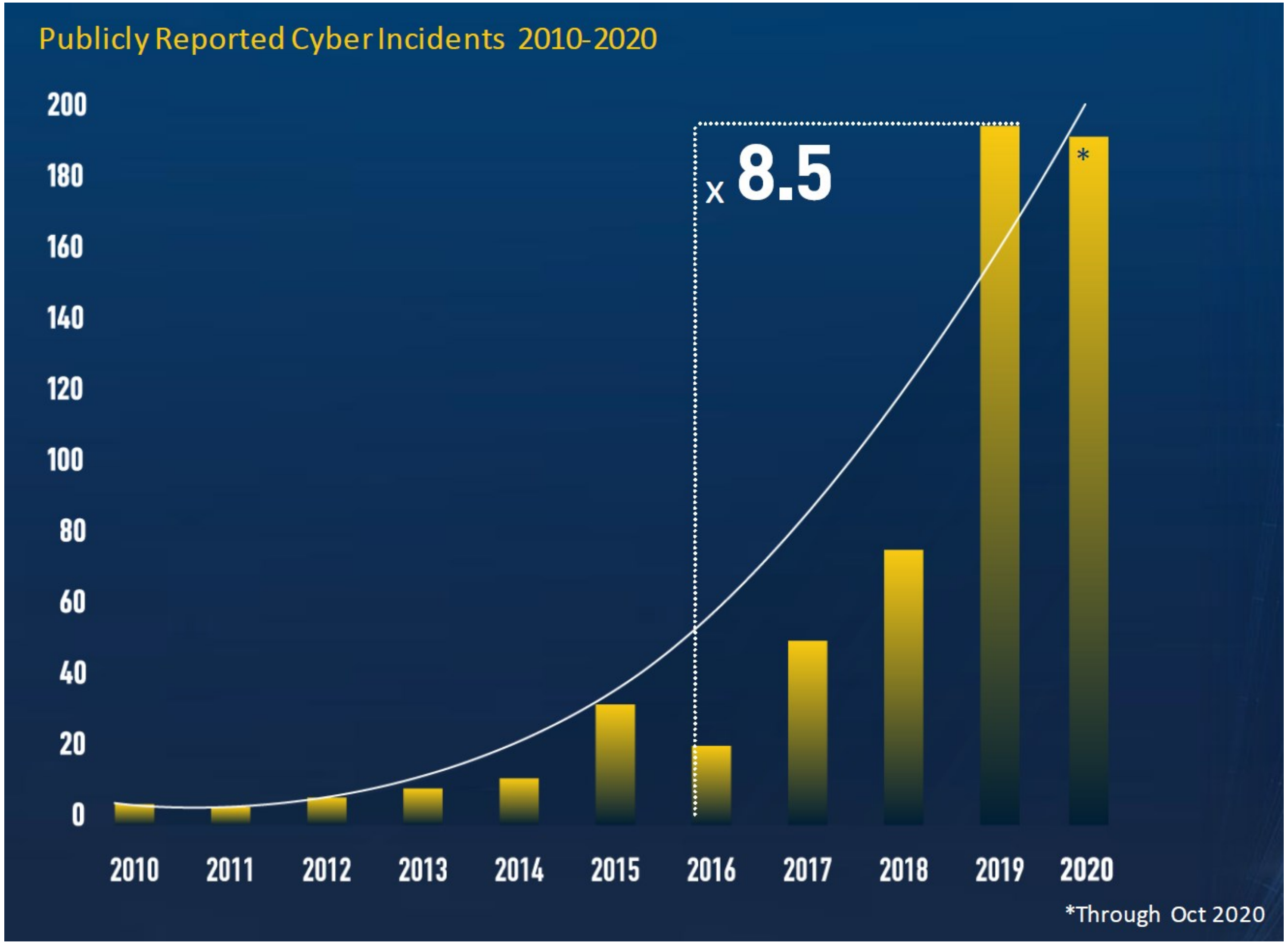
- since 2017 Principal at KUGLER MAAG CIE GmbH
  - Cybersecurity, Functional Safety, ASPICE®, Project Management, Implementation of Security MS, Privacy
  - Process Improvement
  - Risk Management
  - Functional Safety Manager, certified Privacy Commissioner, certified Information Security Commissioner (DGI)
  - intacs certified Provisional Assessor Automotive SPICE
  - professional SCRUM Master
  - Trainer for TÜV NORD-CERTIFIED SECURITY ENGINEER (AUTOMOTIVE)

- before:
  - PhD Computer Science/ Mathematics University of Stuttgart
  - 1993 – 2007 Alcatel•Lucent, several positions
  - 2007 – 2017 ICS AG, Head of Business Unit R&D

- Committees:
  - VDA Cybersecurity
    DIN NA052-00-32-11AK (ISO TC22/SC32/WG11)
  - ZVEI Automotive Cybersecurity
  - Working Group Cybersecurity SPICE intacs™
  - GI working group Privacy by Design

Cybersecurity Automotive – Why Now?

Number of reported Cyber Incidents grow very fast …



[Ups20,App20]

Cybersecurity

Different Terms are often coined, all Facets are needed to implement Security.

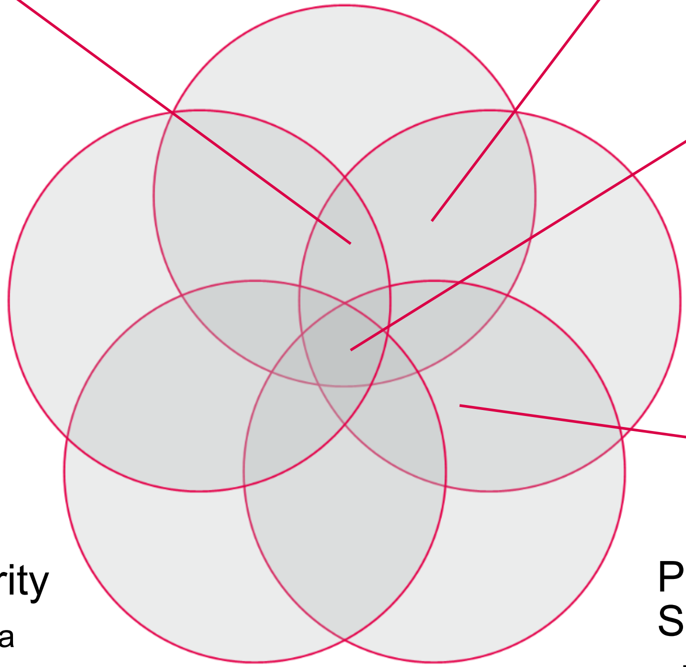
- Telematics backend
- In-Vehicle apps
- Mobile access
- Fleet telematics
- OTA updates
- Service tools

Product Cybersecurity

- Remote access to the vehicle
- Electronic door locks
- ECUs

- Engineering tools
- Threat intelligence

- Key fob
- OBD interface



IT Security

- PKI
- Development infrastructure

Corporate Physical Security

- Insider threat
- Access to IT services

- Physical key cutting Patterns
- Corporate test vehicles

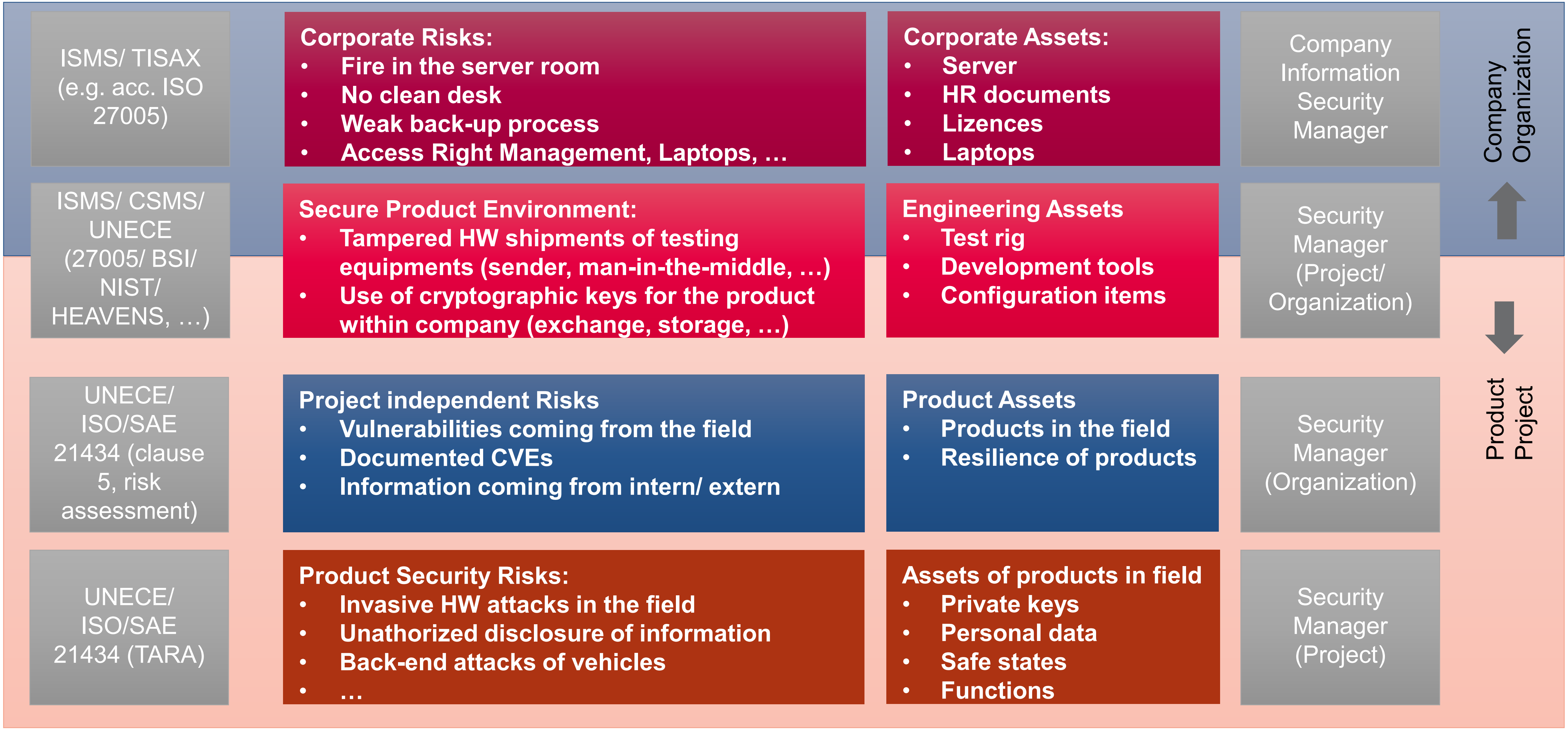
Process Security

- Configuration data
- Production
- Supply chain

Product Physical Security

- Mechanical door locks
- Hood latch

Risk Comparison – Risk Assessment | Roles - Security

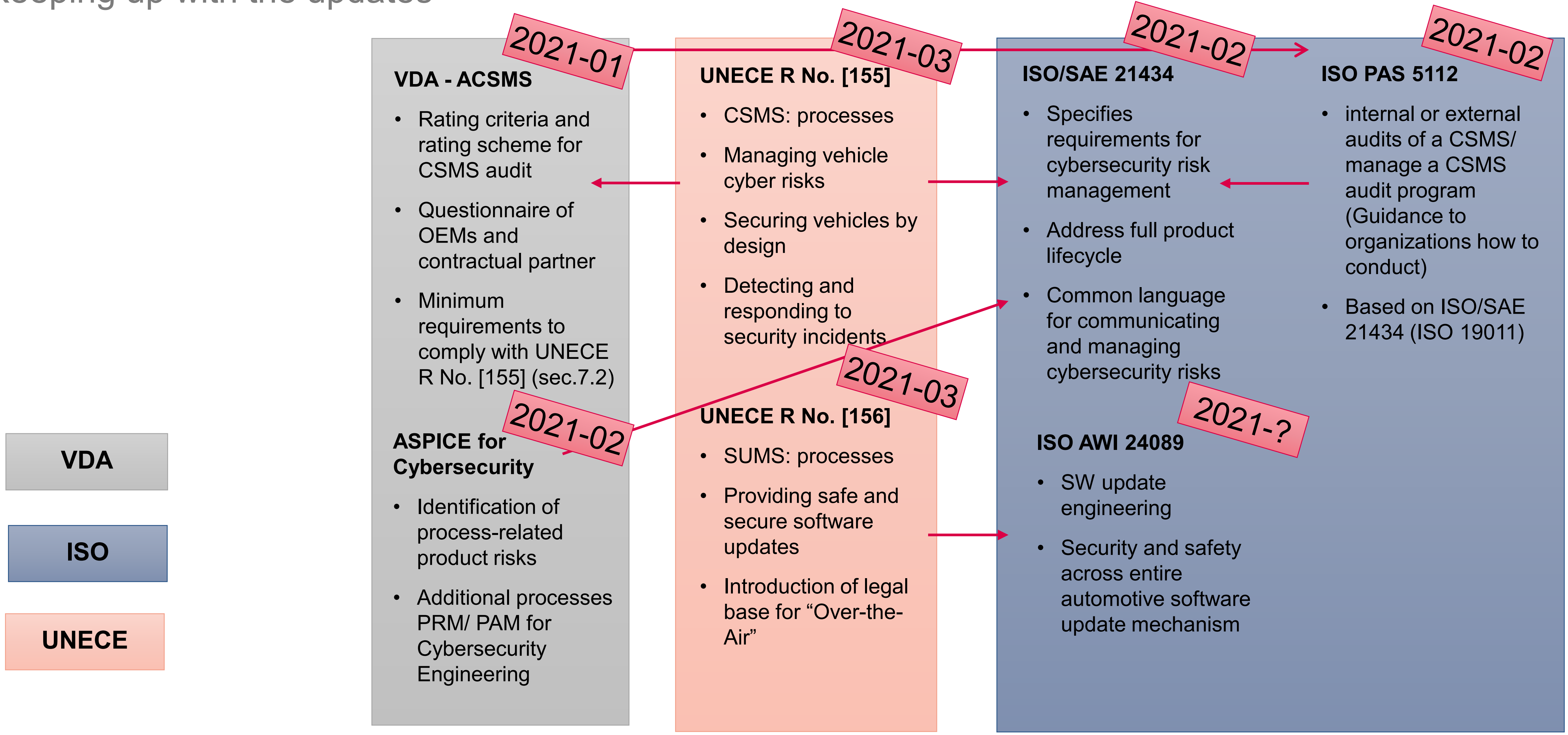


ISMS/ TISAX (e.g. acc. ISO 27005)	**Corporate Risks:** • Fire in the server room • No clean desk • Weak back-up process • Access Right Management, Laptops, …	**Corporate Assets:** • Server • HR documents • Lizences • Laptops	Company Information Security Manager
ISMS/ CSMS/ UNECE (27005/ BSI/ NIST/ HEAVENS, …)	**Secure Product Environment:** • Tampered HW shipments of testing equipments (sender, man-in-the-middle, …) • Use of cryptographic keys for the product within company (exchange, storage, …)	**Engineering Assets** • Test rig • Development tools • Configuration items	Security Manager (Project/ Organization)
UNECE/ ISO/SAE 21434 (clause 5, risk assessment)	**Project independent Risks** • Vulnerabilities coming from the field • Documented CVEs • Information coming from intern/ extern	**Product Assets** • Products in the field • Resilience of products	Security Manager (Organization)
UNECE/ ISO/SAE 21434 (TARA)	**Product Security Risks:** • Invasive HW attacks in the field • Unathorized disclosure of information • Back-end attacks of vehicles • …	**Assets of products in field** • Private keys • Personal data • Safe states • Functions	Security Manager (Project)

Hidden Object

Keeping up with the updates

New version



2021-01

VDA - ACSMS

- Rating criteria and rating scheme for CSMS audit
- Questionnaire of OEMs and contractual partner
- Minimum requirements to comply with UNECE R No. [155] (sec.7.2)

2021-02

ASPICE for Cybersecurity

- Identification of process-related product risks
- Additional processes PRM/ PAM for Cybersecurity Engineering

2021-03

UNECE R No. [155]

- CSMS: processes
- Managing vehicle cyber risks
- Securing vehicles by design
- Detecting and responding to security incidents

2021-03

UNECE R No. [156]

- SUMS: processes
- Providing safe and secure software updates
- Introduction of legal base for “Over-the-Air”

2021-02

ISO/SAE 21434

- Specifies requirements for cybersecurity risk management
- Address full product lifecycle
- Common language for communicating and managing cybersecurity risks

2021-?

ISO AWI 24089

- SW update engineering
- Security and safety across entire automotive software update mechanism

2021-02

ISO PAS 5112

- internal or external audits of a CSMS/ manage a CSMS audit program (Guidance to organizations how to conduct)
- Based on ISO/SAE 21434 (ISO 19011)

VDA

ISO

UNECE

Relevant Safety & Security Standards for Automotive

Overview

ISO/SAE 21434: *Road Vehicles – Cybersecurity Engineering*
- “replacing“ **SAE J3061™ *“Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”.*** Issued 2016-01

UNECE WP.29: CSMS, SUMS | requirements for homologation → **GSR** (**G**eneral **S**afety **R**egulation) requirements for adaption for the EU

VDA QMC ACSMS – ***A**utomotive **C**ybersecurity **S**ecurity **M**anagement **S**ystem (Red Book)*

ISO PAS 5112 – *Road Vehicles – Guidelines for auditing cybersecurity engineering*

VDA QMC ASPICE Extension for Cybersecurity
(Yellow Book)

ISO/AWI 24089 – *Road vehicles — Software update engineering*

NIST SP 800-160 – *Systems Security Engineering*
- Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems

ISO/ IEC-27000-series – *Information technology –Security techniques*
- **TISAX *“Trusted Information Security Assessment Exchange“***

EU Cybersecurity Act: shall increase digital cybersecurity in Europe
- calls on product manufacturers to take appropriate measures to secure their systems against attacks

ENISA (**E**uropean **N**etwork and **I**nformation **S**ecurity **A**gency) *good practices for security of smart cars*

EU-GDPR: ***"EU-G**eneral **D**ata **P**rotection **R**egulation";* Regulation (EU) 2016/679

ISO 20077 *"Road Vehicles -- Extended vehicle (ExVe) methodology".* Issued 2017

ISO 31000:2018 – *Risk Management Guidelines*
- Principles of Risk Management | Terms and definitions

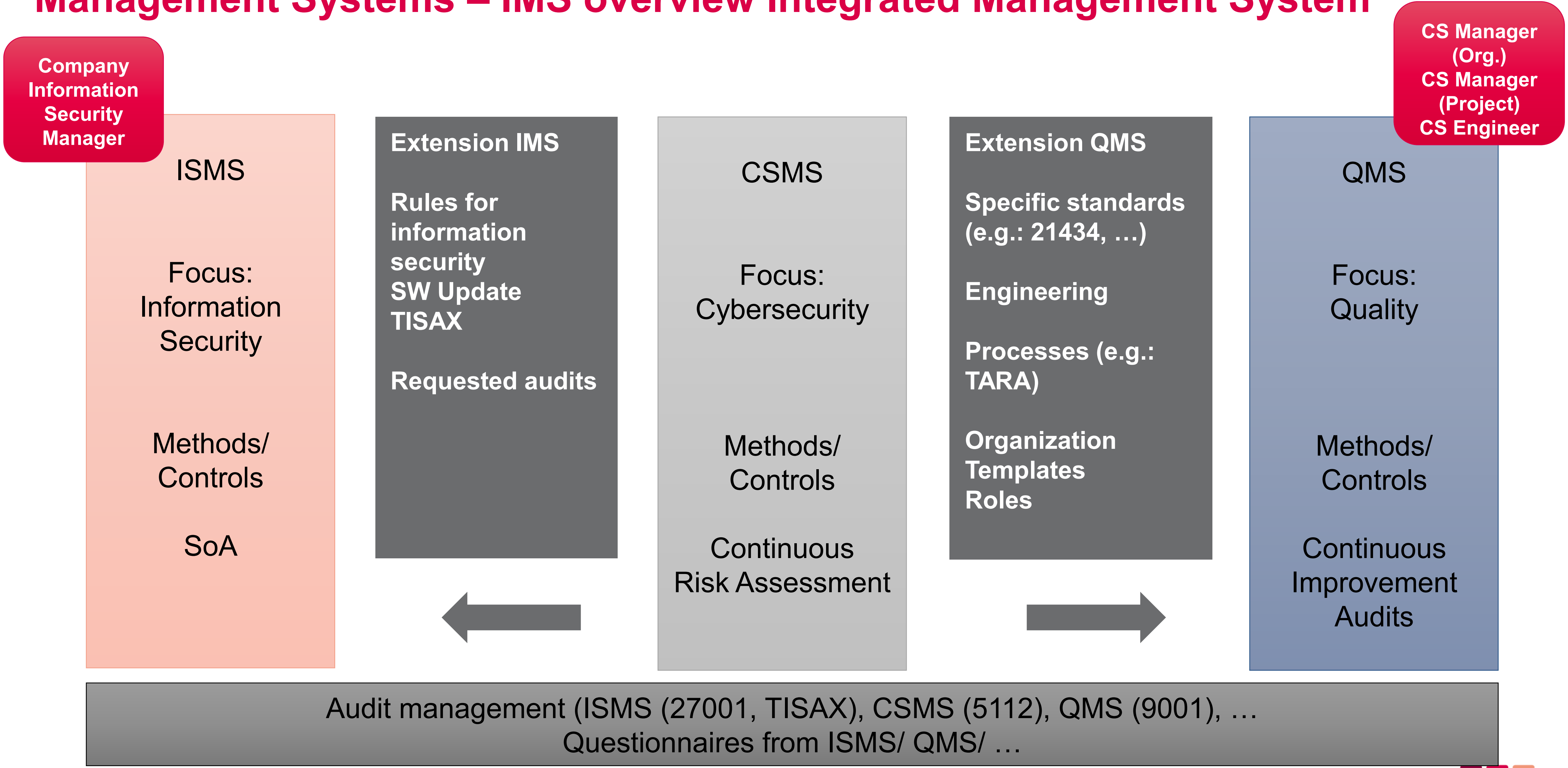
AutoISAC | ***Auto**motive **I**nformation **S**haring and **A**nalysis **C**enter.* Formed in July 2015

ISO 26262:2018 "*Road vehicles – Functional Safety*“ (2nd: edition)

ISO PAS 21448 "*Road vehicles – Safety of the intended functionality*". Issued 2019-01

ISO TR 4804 *“Road vehicles – Safety and cybersecurity for automated driving systems – Design, verification and validation methods”*

Management Systems – IMS overview Integrated Management System



Company Information Security Manager

ISMS

Focus: Information Security

Methods/ Controls

SoA

Extension IMS

Rules for information security
SW Update
TISAX

Requested audits

CSMS

Focus: Cybersecurity

Methods/ Controls

Continuous Risk Assessment

Extension QMS

Specific standards (e.g.: 21434, …)

Engineering

Processes (e.g.: TARA)

Organization
Templates
Roles

CS Manager (Org.)
CS Manager (Project)
CS Engineer

QMS

Focus: Quality

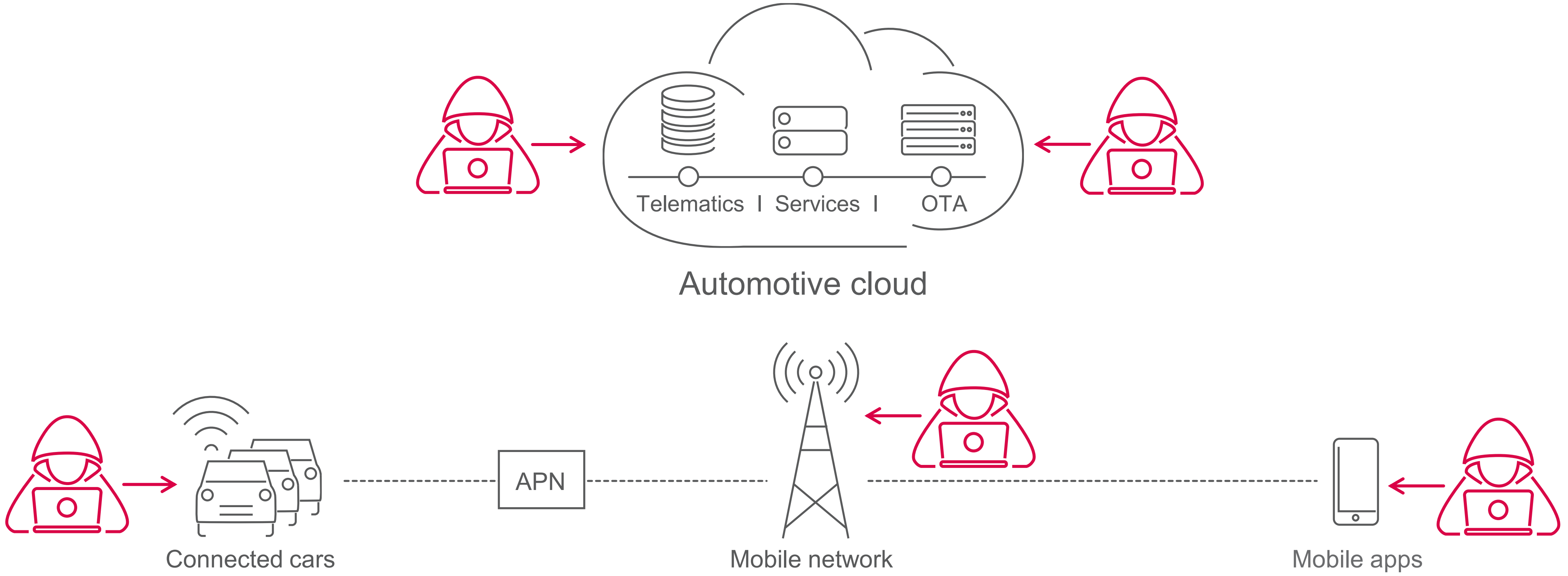
Methods/ Controls

Continuous Improvement Audits

Audit management (ISMS (27001, TISAX), CSMS (5112), QMS (9001), …
Questionnaires from ISMS/ QMS/ …

UNECE regulation No. [155] – ANNEX 5 – Threats and potential Attacks

- Backend servers
- Update procedures
- Unintended human actions
- External connectivity
- Vehicle communications channel
- Threats to vehicle data/code
- Additional vulnerabilities



Telematics I Services I OTA

Automotive cloud

APN

Connected cars

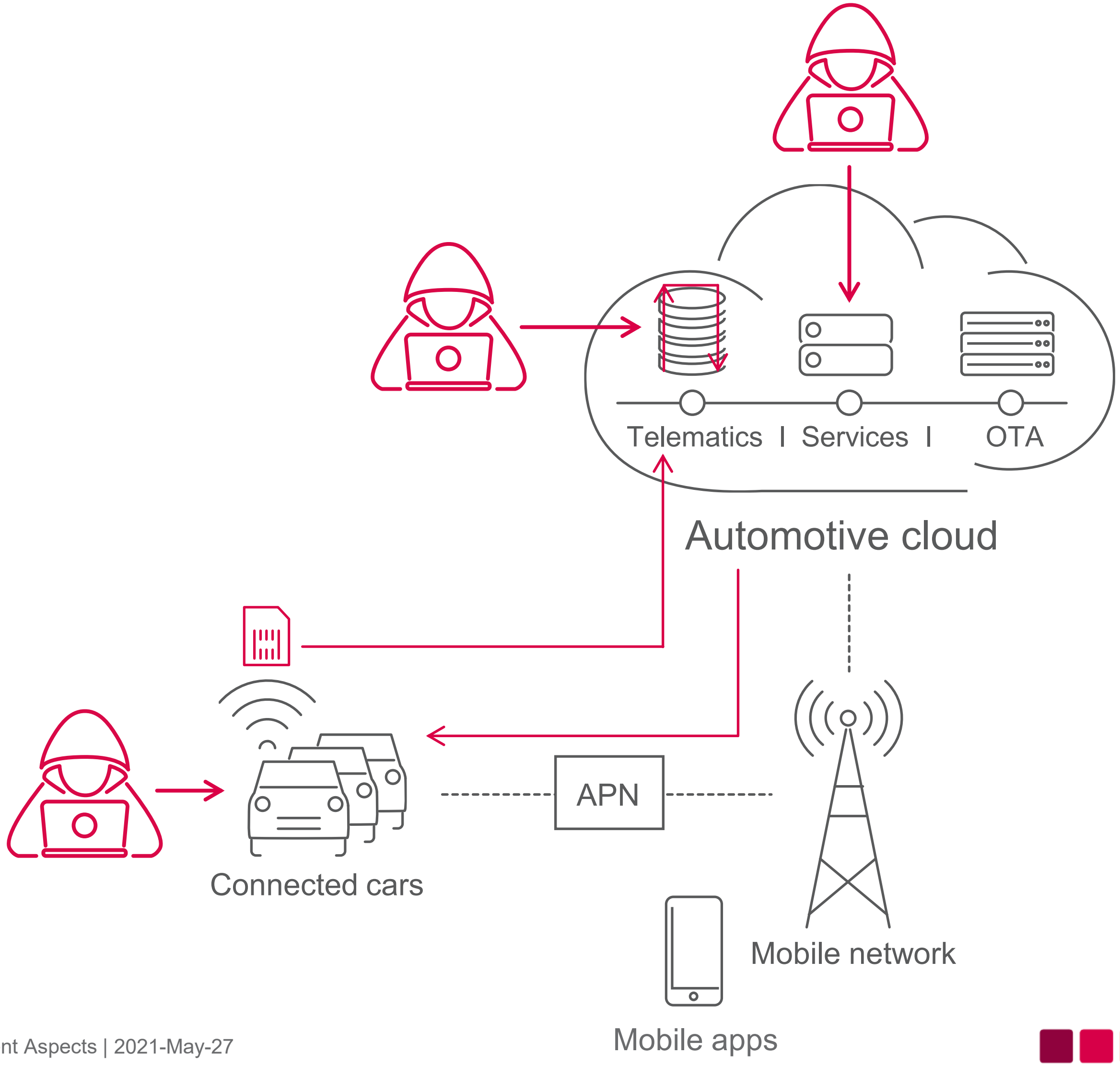
Mobile network

Mobile apps

The Tables of Part A list grouped Threats with Examples

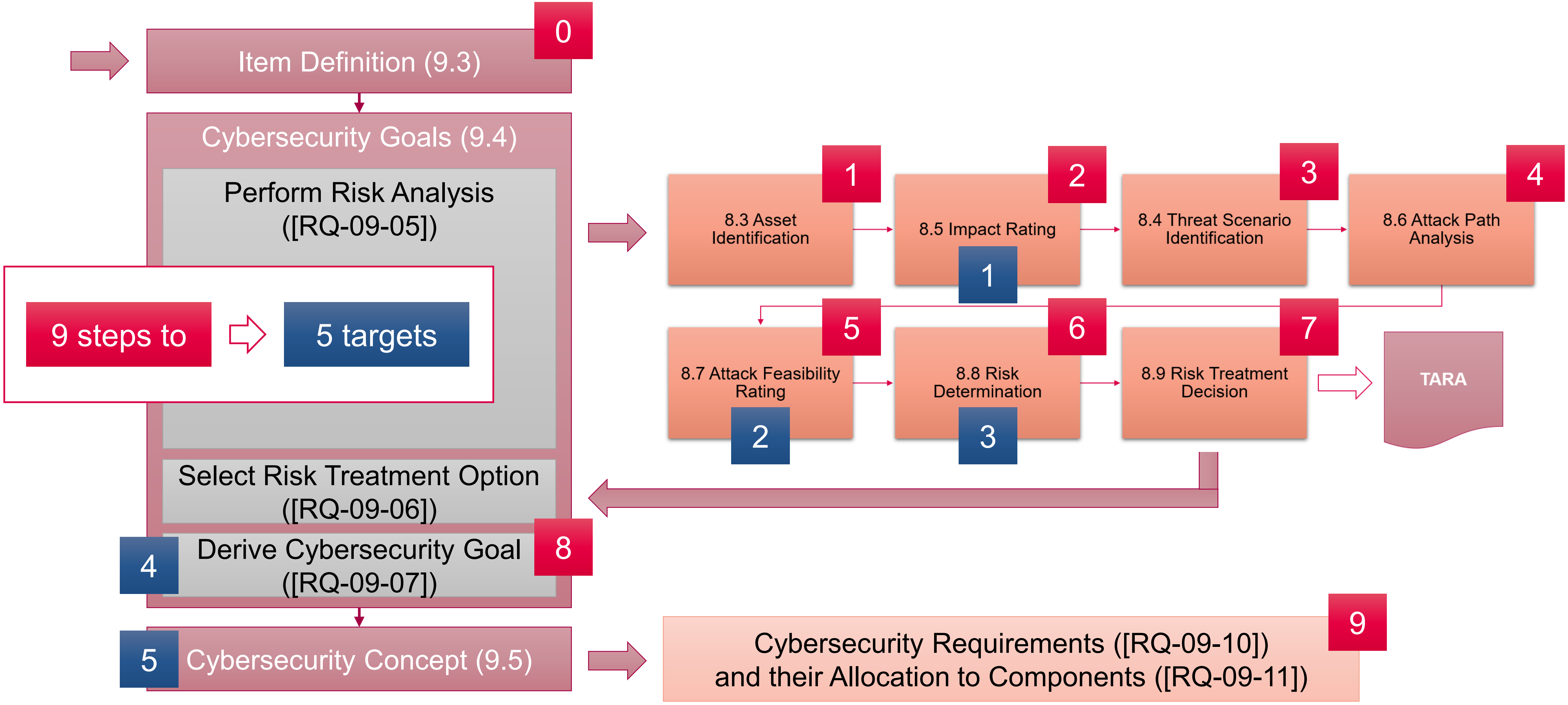
Back-end Servers related to Vehicles in the Field

- Back-end servers used as a means to attack a vehicle or extract data
  - Abuse of privileges by staff (insider attack)
  - Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
  - Unauthorized physical access to the server (conducted by for example USB sticks or other media connecting to the server)
- Services from back-end server being disrupted, affecting the operation of a vehicle
  - Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on
- Vehicle related data held on back-end servers being lost or compromised (“data breach”)
  - Abuse of privileges by staff (insider attack)
  - Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers
  - Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
  - Unauthorized physical access to the server (conducted for example by USB sticks or other media connecting to the server)
  - Information breach by unintended sharing of data (e.g., admin errors)



Steps Item Definition till Cybersecurity Requirement

Requirements and Recommendations | Nine2Five



0 Item Definition (9.3)

Cybersecurity Goals (9.4)

Perform Risk Analysis ([RQ-09-05])

9 steps to

5 targets

Select Risk Treatment Option ([RQ-09-06])

4 Derive Cybersecurity Goal ([RQ-09-07]) 8

5 Cybersecurity Concept (9.5)

1 8.3 Asset Identification

2 8.5 Impact Rating 1

3 8.4 Threat Scenario Identification

4 8.6 Attack Path Analysis

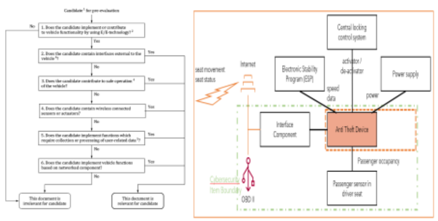
5 8.7 Attack Feasibility Rating 2

6 8.8 Risk Determination 3

7 8.9 Risk Treatment Decision

TARA

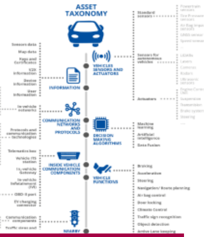
9 Cybersecurity Requirements ([RQ-09-10]) and their Allocation to Components ([RQ-09-11])



Checklists

ENISA (A)

HARA



Confidentiality
Integrity
Availability
Authenticity
Non-repudiation
Authorization

MS-STRIDE

	Authenticity	Integrity	Non-repudiation	Confidentiality	Availability	Authorization
External Entity	x		x			
Data Flow		x		x	x	
Data Store		x	x	x	x	
Process	x	x	x	x	x	x

legend for pattern:
red: minimum description to be mentioned (mandatorily)
black: additional text/ explanation (optional)
blue: explanation with reference to the left (optional)

Item definition → Asset Enumeration → Cybersecurity Properties → Damage Scenario Identification

Road User
Fleet Manager
OEM

Table 1 — Classes of severity

	Class			
	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Impact Level
Severe
Major
Moderate
Negligible

HEAVENS

CVSS

EVITA

Elapsed Time	Specialist Expertise	Knowledge of the item	Window of opportunity	IT hardware/software of other equipment required	Elapsed Time	Specialist Expertise	Knowledge of the item	Window of opportunity	IT hardware/software of other equipment required	Total Value	Attack feasibility Value
≤ 3 years	Expert	Sensitive	Moderate	Specialised	10	6	7	4	4	31	Very low
< 6 months	Proficient	Restricted	Moderate	Specialised	4	3	3	4	4	18	Medium
< 6 months	Proficient	Senstive	Moderate	Standard	4	3	7	4	0	18	Medium
≤ 3 years	Proficient	Sensitive	Easy	Standard	10	3	7	1	0	21	Low
< 6 months	Proficient	Restricted	Moderate	Specialised	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
< 1 month	Proficient	Restricted	Moderate	Standard	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Level
High
Medium
Low
Very low

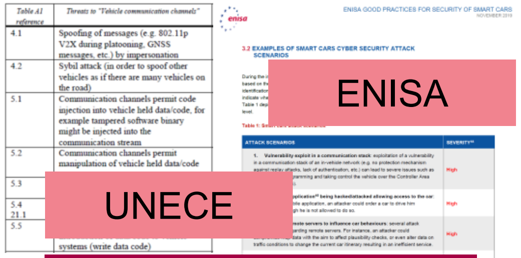


Table A1 reference | Threats to "Vehicle communication channels"

4.1 Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation
4.2 Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)
5.1 Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream
5.2 Communication channels permit manipulation of vehicle held data/code
5.3
5.4
21.1
5.5
systems (write data code)

ENISA GOOD PRACTICES FOR SECURITY OF SMART CARS

3.2 EXAMPLES OF SMART CARS CYBER SECURITY ATTACK SCENARIOS

ENISA

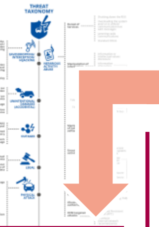
UNECE

STRIDE
Threats
Spoofin
Tamperi
Repudiat
Information Disclosure
Denial of
Elevation of Privilege

UNECE

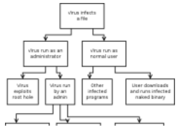
MS-STRIDE

ENISA (B)



Attack Feasibility Rating ← Attack Path Analysis ← Threat Scenario Identification

Impact Rating
S - FOP



ATA

MITRE

ISO 26262

Stakeholder: Road User				Stakeholder: OEM		
S	F	O	P	F_{OEM}	O_{OEM}	P_{OEM}
2	0	3	0	1	3	0
2	0	3	0	1	3	0
2	0	3	0	1	3	0

		Attack Feasibility			
		Very Low	Low	Medium	High
Impact	Severe	2	3	4	5
	Major	2	3	3	4
	Moderate	2	2	2	3
	Negligible	1	1	1	2

X

Risk Determination

Impact Analysis															
Stakeholder: Road User				Stakeholder: O											
S	F	O	P	F_{OEM}	O_{OEM}	P_{OEM}	Value	Attack feasibility	S	F	O	P	F_{OEM}	O_{OEM}	P_{OEM}
3	0	3	0	1	3	0	31	Very low	1	1	1	1	[illegible]	[illegible]	1
3	0	3	0	1	3	0	18	Medium	4	1	4	1	[illegible]	[illegible]	[illegible]
3	0	3	0	1	3	0	18	Medium	4	1	4	1	2	4	1
0	0	0	1	3	0	2	21	Low	1	1	1	2	3	1	2
0	0	2	0	0	1	0	18	Medium	1	1	3	1	1	2	1
3	0	3	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	High	5	[illegible]	5	1	[illegible]	[illegible]	1

Risk Treatment
Avoiding
Reducing
Sharing
Accepting

Risk Treatment Decision	Clause 8 Requirement	Clause 9 Requirement	consequence in concept phase
Avoidance	RQ-08-12	RQ-09-06, Note 7	re-iteration of concept phase
Reducing		RQ-09-07	specification of cybersecurity goal(s)
Acceptance		RQ-09-08	statement of cybersecurity claim(s)
Sharing/ transfering			

Risk Treatment Decision

Cybersecurity Claims

Risk Treatment decision	
Option taken	Controls/ Remarks/ Cybersecurity Goal
reducing the risk (e.g. implementation of controls)	CG01: during driving it has to be checked regularily if seat sensor is sending "occupied"
accepting or retaining the risk	risk is very low, can be accepted
reducing the risk (e.g. implementation of controls)	CG02: add reshness values (e.g. message counter, PRNG, ...) to the seat sensor messages to avoid replay attacks
sharing or transferring the risk (e.g. through contracts, buying insura[illegible]	sharing with an insurance, financial impact will be only on OEMs side
accepting or re[illegible]	[illegible]
[illegible] or re[illegible]	[illegible]

Cybersecurity Goals

ENISA (C)

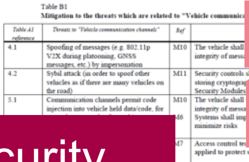
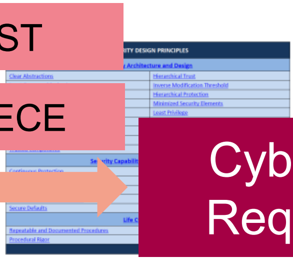


Table B1
Mitigation to the threats which are related to "Vehicle communication channels"

NIST

UNECE



Cybersecurity Concept

GOOD PRACTICES

Cybersecurity Requirements

Thank you

Thomas Liedtke (PhD)
+49 173 676 40 93
Thomas.liedtke@kuglermaag.com
www.kuglermaag.com

KUGLER MAAG CIE
besser mit uns