Latest News from Automotive Safety & Cybersecurity Standards

FuSaCom, 25.G2G am 28.09.2020

Erwin Schoitsch, AIT Austrian Institute of Technology

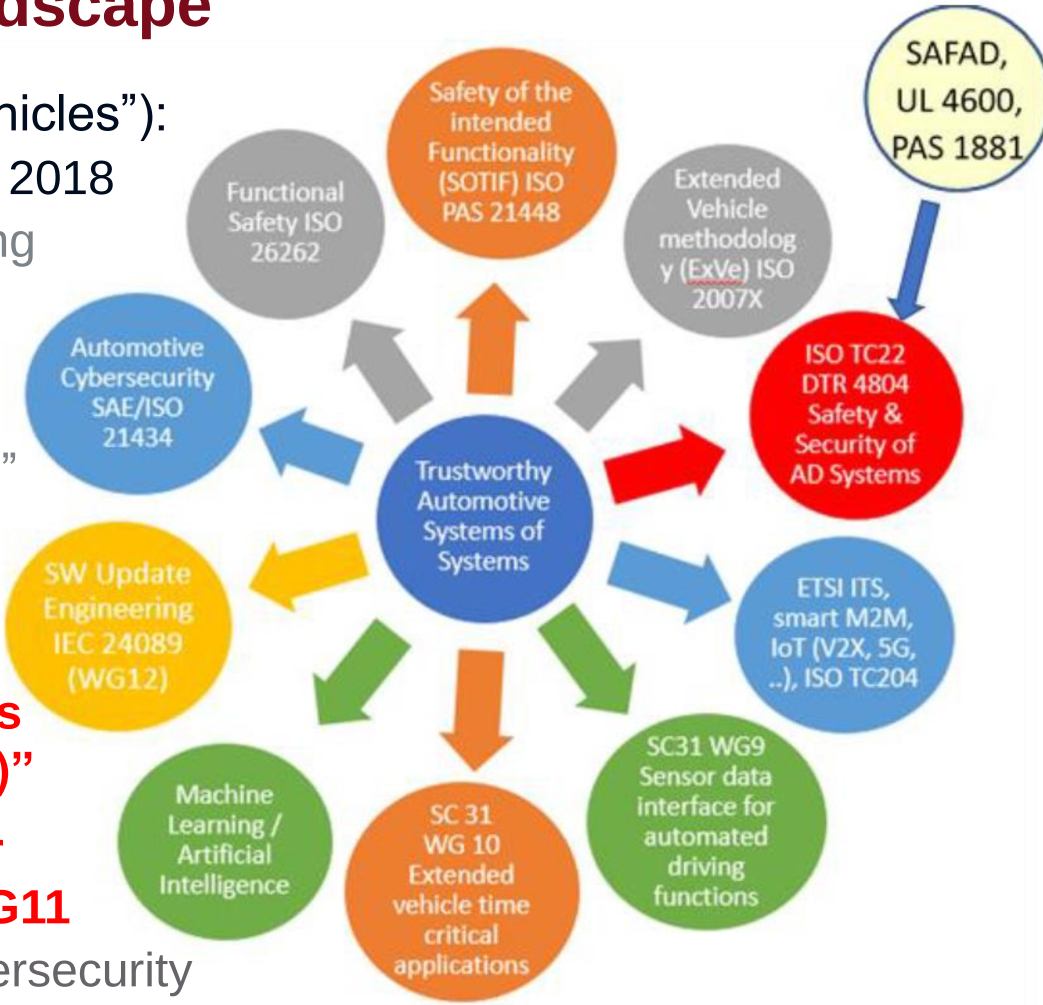
Agenda

- The Automotive Standardization Landscape – ISO TC22
- Status ISO DIS 21434 und Cybersecurity Audit Guideline ISO PAS 5112
- UNECE Cybersecurity Regulations (Proposals) und ISO 24089 (Software Update engineering)
- ISO TR 4609 (published July 2020) - Road vehicles — Report on standardisation prospective for automated vehicles (RoSPAV)
- ISO TR 4804, Final (July 2020) - Safety and cybersecurity for automated driving systems – Design, verification and validation methods (main focus 1)
- The other side – ISO TC204 ITS Intelligent transport systems
- Outlook: SECREDAS standardization strategy – helping to bring ExVe and ITS together

Automotive Standardization Landscape

Safety: TC22 SC32 WG8 ("Road vehicles"):

- ISO 26262 => Edition 2 publ. end of 2018
  - Interface to cybersecurity, including bus and trucks, separate part for semiconductors and motorcycles – now: collection of experiences from NCs to find the "way forward"
- ISO PAS 21448 => Safety standard aimed at automated functions
  - Nominal safe behavior → **Updating/Enhancement towards "Full International Standard (IS)"**



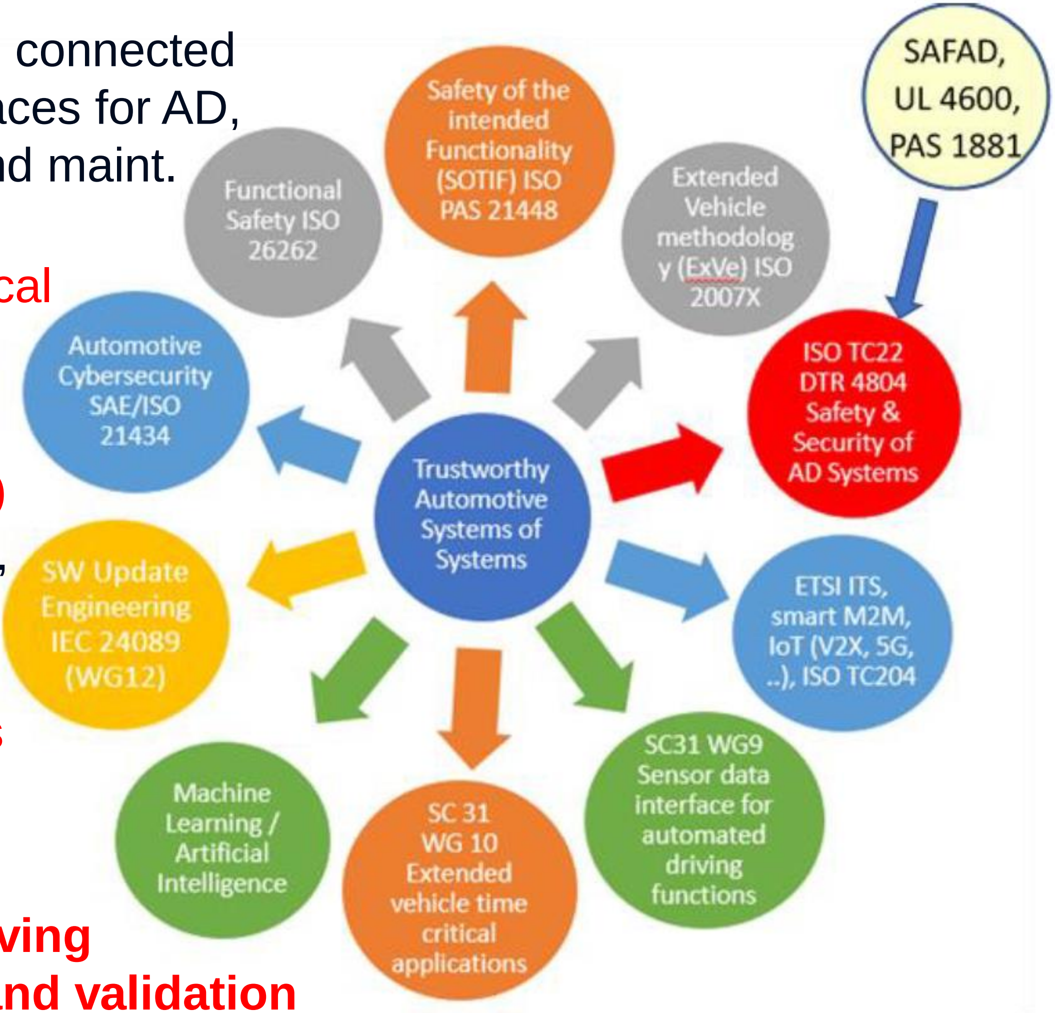
SAFAD, UL 4600, PAS 1881
Safety of the intended Functionality (SOTIF) ISO PAS 21448
Functional Safety ISO 26262
Extended Vehicle methodology (ExVe) ISO 2007X
Automotive Cybersecurity SAE/ISO 21434
Trustworthy Automotive Systems of Systems
ISO TC22 DTR 4804 Safety & Security of AD Systems
SW Update Engineering IEC 24089 (WG12)
ETSI ITS, smart M2M, IoT (V2X, 5G, ..), ISO TC204
Machine Learning / Artificial Intelligence
SC 31 WG 10 Extended vehicle time critical applications
SC31 WG9 Sensor data interface for automated driving functions

Automotive Cybersecurity (Basis for UNECE Regulations): TC22 SC32 WG11

- ISO/SAE 21434 => Automotive Cybersecurity Engineering (**DIS** !) - Engineering of secure systems,
- **NEW: PAS 5112 Guidelines for auditing cybersecurity engineering (Lead: AIT)**
- **WG12: Software Update engineering – OTA** (concept re-evaluated, work restructured)

Automotive Standardization Landscape

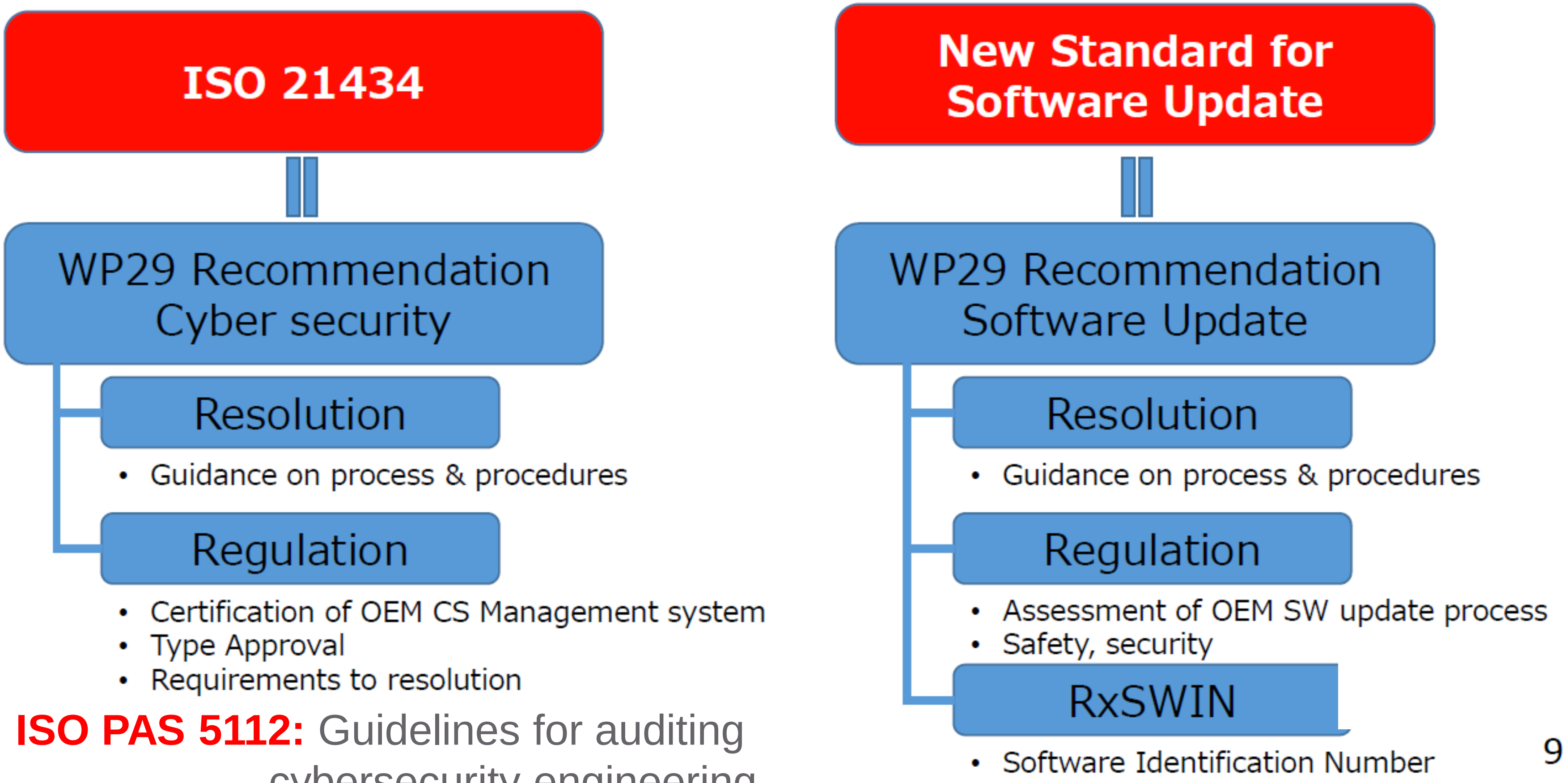
- **ISO TC22 SC31** extended Vehicle, connected car communications, sensor interfaces for AD, remote diagnosis, remote repair and maint. (RMI), web services, V2X, V2Grid
- WG10, Extended Vehicle time-critical applications – RExVeS ISO 23132
- **NEW:** ISO TC22 AHG1 ADAG (Automated Driving Ad-Hoc Group)
- many *sub-committees* coordinated, goal: roadmap
- ISO TR 4609 Report on stand. prospective for automated vehicles (RoSPAV) → ISO TC22 & TC 204


SAFAD,
UL 4600,
PAS 1881
Safety of the intended Functionality (SOTIF) ISO PAS 21448
Functional Safety ISO 26262
Extended Vehicle methodology (ExVe) ISO 2007X
Automotive Cybersecurity SAE/ISO 21434
Trustworthy Automotive Systems of Systems
ISO TC22 DTR 4804 Safety & Security of AD Systems
SW Update Engineering IEC 24089 (WG12)
ETSI ITS, smart M2M, IoT (V2X, 5G, ..), ISO TC204
Machine Learning / Artificial Intelligence
SC 31 WG 10 Extended vehicle time critical applications
SC31 WG9 Sensor data interface for automated driving functions

- **NEW: ISO TR 4804 "Safety and cybersecurity for automated driving systems – Design, verification and validation methods" (Kick-off Feb. 2020, Published July 2020)** <related: **White Paper "Safety First for AD – SAFAD", UL 4600 (US), PAS 1881 (BSI)**> → **"Twelve Principles of AD"**

Automotive Cybersecurity Standards

WG12 ISO/NP 24089 Software Update standard (OTA) (members!), ONGOING



ISO 21434

WP29 Recommendation Cyber security

Resolution

- Guidance on process & procedures

Regulation

- Certification of OEM CS Management system
- Type Approval
- Requirements to resolution

New Standard for Software Update

WP29 Recommendation Software Update

Resolution

- Guidance on process & procedures

Regulation

- Assessment of OEM SW update process
- Safety, security

RxSWIN

- Software Identification Number

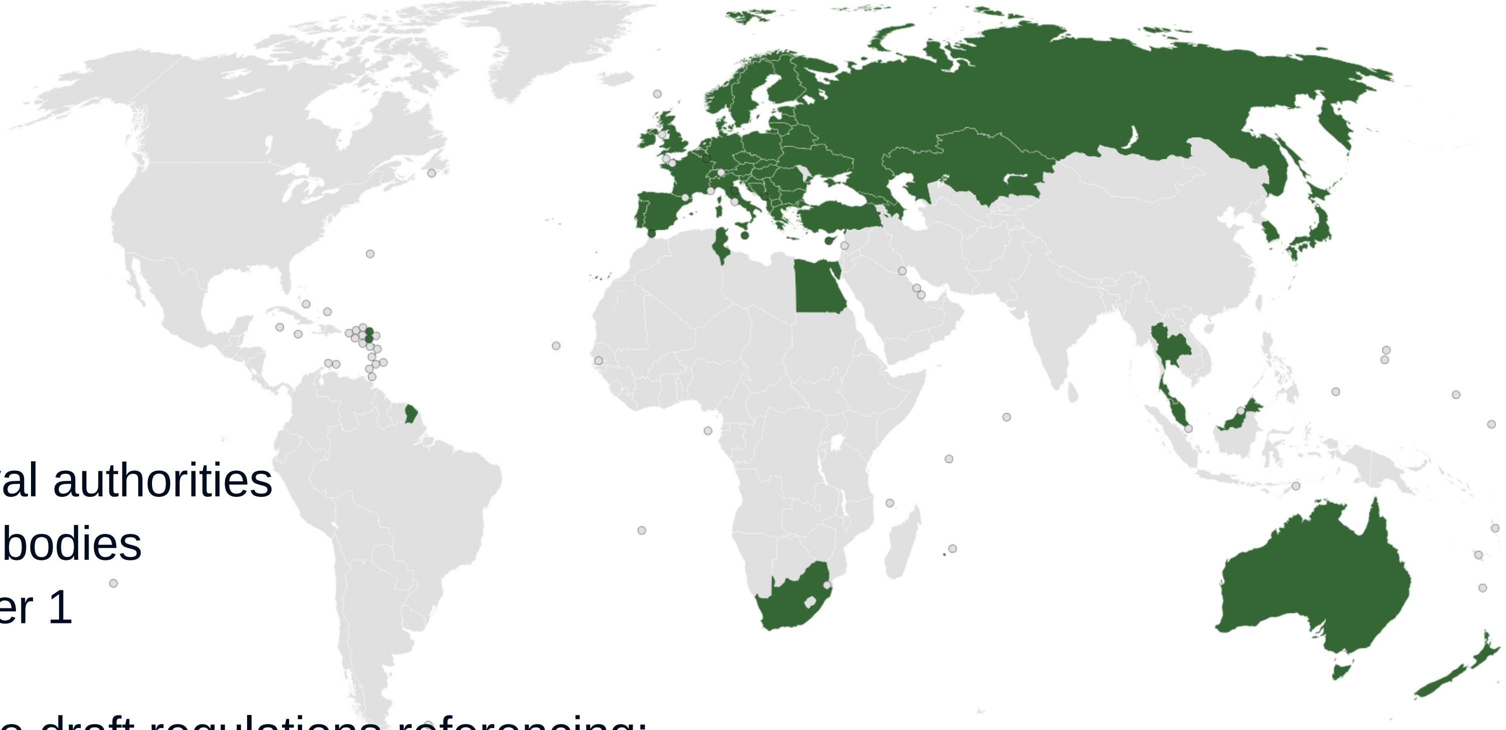
9

ISO PAS 5112: Guidelines for auditing cybersecurity engineering

Automotive Regulation: ISO/SAE 21434 and Software Update Engineering **highly relevant** – already cited in the upcoming regulations of **UN-ECE on Cybersecurity and Software Updates over the Air! (Requirement: Cybersecurity Management System covering the whole supply chain!)**

UNECE World Forum for Harmonization of Vehicle Regulations

UNECE WP29 defines requirements for type approval



UNECE addresses Cyber Security

Main requirement: Security Management System covering the whole supply chain

Members are:

- Type approval authorities
- Certification bodies
- OEM and Tier 1

- Delivered two draft regulations referencing:
  - Cyber Security → ISO/SAE 21434
  - **Audit guideline → ISO PAS 5112 belongs to implementation of ISO/SAE 21434 (lead: AIT) (CS Management System covering whole supply chain)**
  - Software updates → ISO 24089 planned

→ **Strong impact of these standards!** Impact beyond the member states,

ISO TC22 AG1
Automated driving ad hoc group

Contributions from: SC31, SC32, SC33 (ADAS), SC35, SC37, SC39
Contacts to: TC 204 (ITS), TC 241 (Road safety), SAE, (ETSI, CEN/CLC)
Example: SC31, Data communication – incl. Extended Vehicle, Connected Car

SC 31 - Data communication
Alternate Chairs: J Bräuninger (DE), N Morand (FR)
Secretary: E Wern (DE)

JWG1 - Vehicle to grid communication interface
Conv: P Bertrand
Sec: E Wern

WG2 - Vehicle diagnostic protocols
Conv: G Feiter
Sec: E Wern

WG3 - In-vehicle networks
Conv: H Zeltwanger
Sec: E Wern

WG4 - Network applications
Conv: H Zeltwanger
Sec: E Wern

WG5 - Test equipment/Data eXchange Formats
Conv: T Malaterre
Sec: F Martin

WG6 - Extended vehicle / Remote diagnostics
Conv: J-F Renaudin
Sec: V Maupin

WG7 - Electronic periodic technical inspection
Conv: T Raith
Sec: E Wern

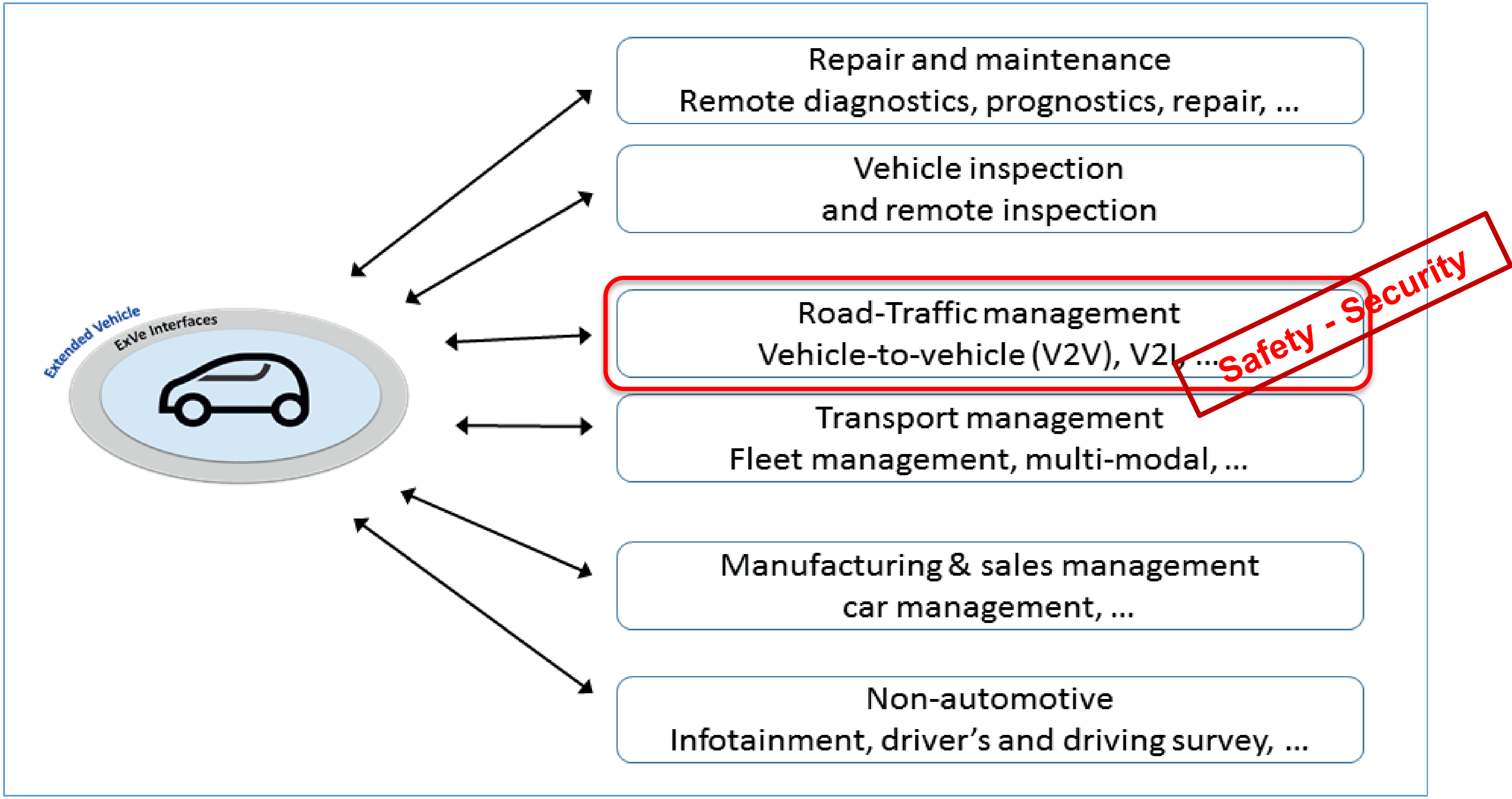
WG8 - Vehicle domain - Data collection system
Conv: K Tokita
Sec: K Takano

WG9 - Sensor data interface for automated driving functions
Conv: T Schaller
Sec: E Wern

WG10 - Peri-vehicular data communication
Conv: T Malaterre
Sec: V Maupin

ISO TC22 SC31 – Data Communications (V2X) Extended Vehicle Use Case Clusters

(list non-exhaustive) – concerns “Connected vehicle” from different view points
→ e.g. **new for AD**: WG 10 on “Extended vehicle time critical applications”



Repair and maintenance
Remote diagnostics, prognostics, repair, …

Vehicle inspection
and remote inspection

Road-Traffic management
Vehicle-to-vehicle (V2V), V2I, …

Safety - Security

Transport management
Fleet management, multi-modal, …

Manufacturing & sales management
car management, …

Non-automotive
Infotainment, driver’s and driving survey, …

ISO CD 23132 Time constrained peri-vehicular data communications for the Extended Vehicle (ExVe)

General requirements, definitions and use cases related to Road and ExVe Safety (**RExVeS**) (2019)

Definition: "entity, still in accordance with the specifications of the vehicle manufacturer, that extends beyond the physical boundaries of the road vehicle and consists of the road vehicle, off-board systems, external interfaces, and the data communication between the road vehicle and the off-board systems".

Goal: „contribute to road safety … e.g. by reducing the number of road fatalities through collision avoidance cooperation"

ExVe Time Critical interfaces: are firstly associated with safety-critical functions (e.g. emergency braking, steering, ...) that are functions for which the priorities are based on a criticality concept.

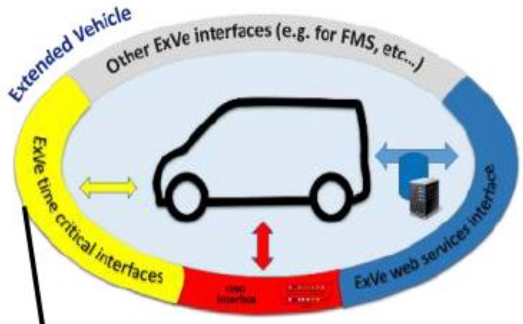
Concept: Situation-based (scenario) Risk/Hazard Analysis**,** Determination of the **priority class** (criticality) of a **RExVeS-related time-constrained situation**

Priority Class (1-6): determined by "Severity" (0-4, no injuries to fatality for community), Exposure class (Probability 1-4, very low to high) and "Controllability" (1-3, simple to difficult)

ISO CD 23132 (RExVeS)

RExVeS Methodology in context of ExVe Design methodology: Scenario analysis and classification of situations → derive requirements for time constrained safety-related functions

Typical interfaces of an extended vehicle (from ISO 20077-1:2017)

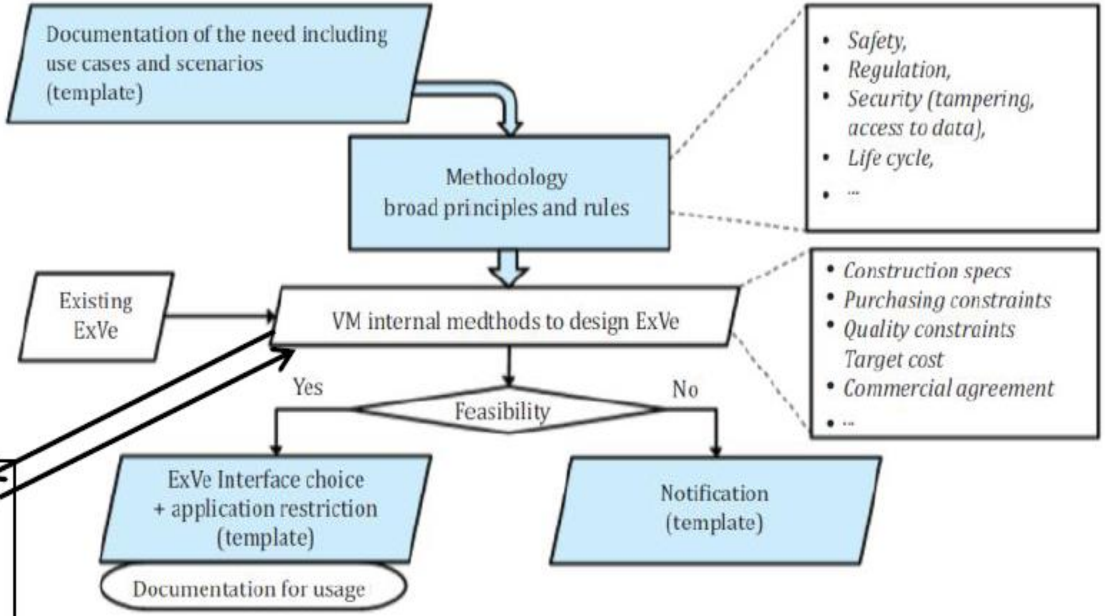

Extended Vehicle
Other ExVe interfaces (e.g. for FMS, etc...)
ExVe time critical interfaces
ExVe web services interface
OBD interface

If ExVe time critical interfaces are considered

ISO 23132 RExVeS Methodology

- Design prerequisites
- Analysis of scenarios
- Classification of situations

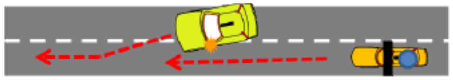
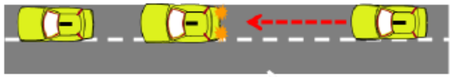
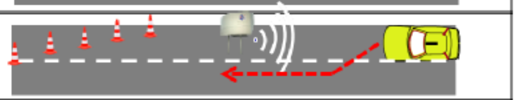
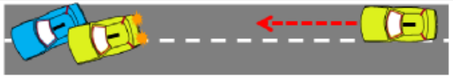
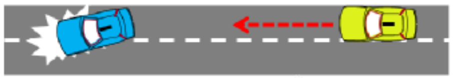
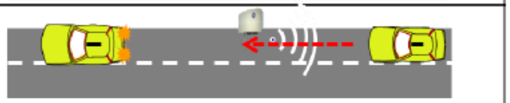
Schematic of the ExVe design methodology context (from ISO 20077-2:2018)

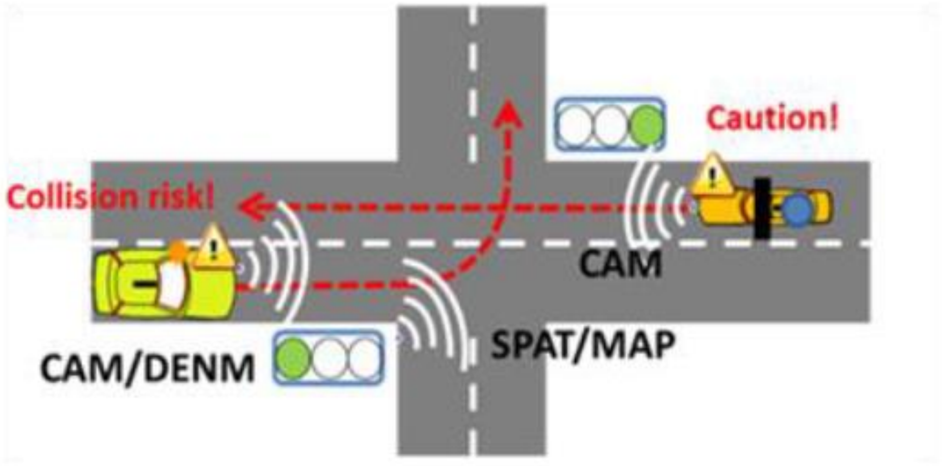

Documentation of the need including use cases and scenarios (template)
Methodology broad principles and rules
• Safety,
• Regulation,
• Security (tampering, access to data),
• Life cycle,
• ...
Existing ExVe
VM internal medthods to design ExVe
• Construction specs
• Purchasing constraints
• Quality constraints
Target cost
• Commercial agreement
• ...
Yes
Feasibility
No
ExVe Interface choice + application restriction (template)
Documentation for usage
Notification (template)

Different from SotiF: Whole life cycle, regulations, safety and security considered

ISO CD 23132 (RExVeS)

Scenarios taken from ETSI ITS TS 101 539-1, 2 and 3 (Road hazard and collision warnings), e.g. list of use cases (examples)

Use case	Scenario illustration
Safety relevant lane Change	
Emergency electronic brake light / Traffic condition	
Roadworks	
Stationary vehicle	
Stability problem	
Collision risk warning from a third party	



Hazardous locations:

- ✓ Slow/stationary vehicle(s) & Traffic ahead warning
- ✓ Road works warning
- ✓ Weather conditions
- ✓ Emergency brake light
- ✓ Emergency vehicle approaching
- ✓ Other hazardous notifications
- ✓ Vulnerable Road user protection

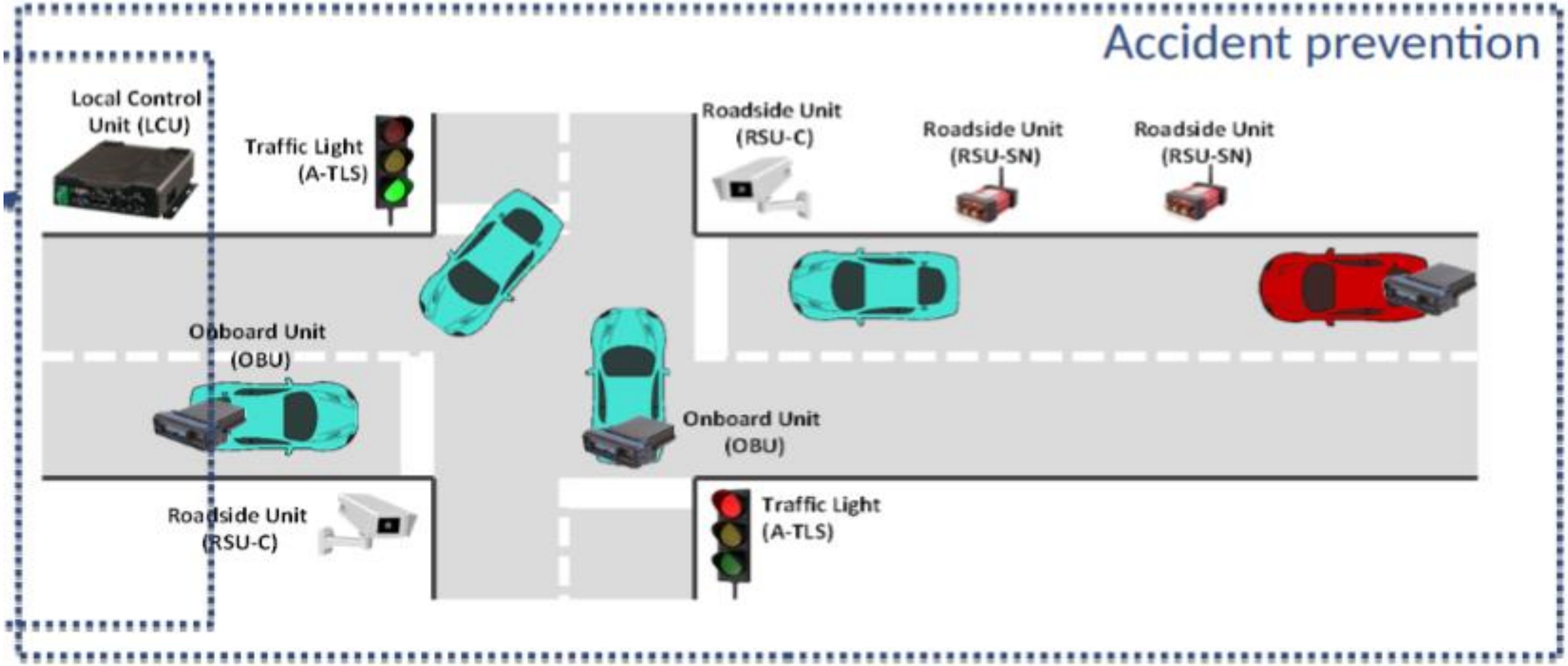
Signalling applications and others

- ✓ In-vehicle signage
- ✓ In-vehicle speed limits
- ✓ Signal violation/intersection safety
- ✓ Traffic signal priority
- ✓ Green Light Optimal Speed Advisory
- ✓ Local hazard warning
- ✓ Connected/Cooperative navigation
- ✓ Parking and Traffic Guidance

Future Topics
"Trustworthiness", "Swarm intelligence""

Study group AHG19, in ISO/IEC JTC1 SC41

- Automotive USE CASES with cooperative CPS/SoS planned (Proj. SAFECOP):
  (1) Planned: Swarm intelligence and ITS - Input to the report
  (2) Collaborative vehicles and Infrastructure optimizing overall regional traffic by swarm intelligence and collaborative CPS

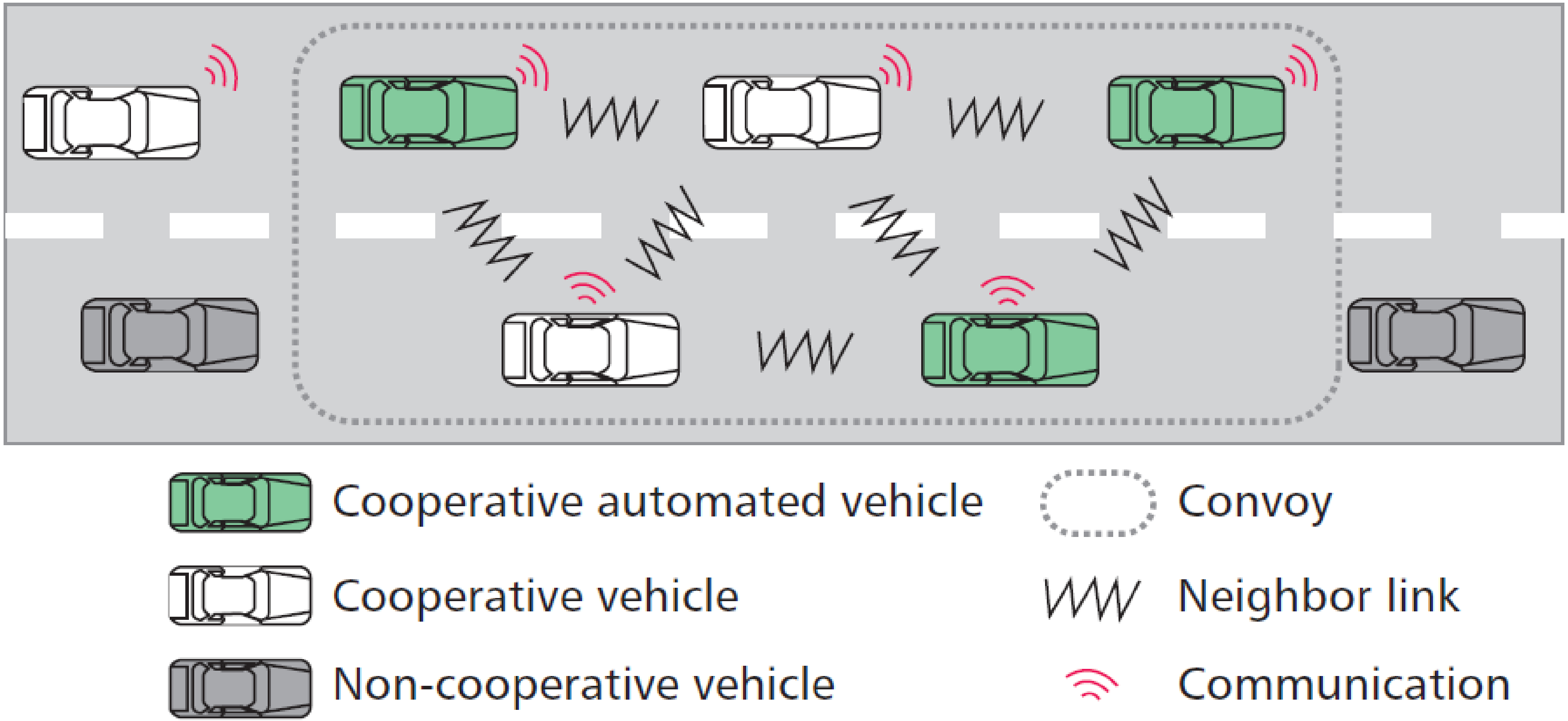


(unfortunately disbanded 2019)

Future Topics
“Trustworthiness”, “Swarm intelligence”„

Study group AHG19, in ISO/IEC JTC1 SC41

- Automotive USE CASES with cooperative CPS/SoS planned (Proj. SAFECOP): (3) Cooperative vehicles in optimized autonomous driving (dual-lane platooning with connected non-automated and automated vehicles)



(unfortunately disbanded 2019)

ISO TC22 AG1
Automated driving ad hoc group

ISO TR 4906 Report on standardization prospective for automated vehicles (RoSPAV)

Key contents:

- List of current projects and standards (SC 31, SC32, SC 33, SC 35, SC37, SC39) and taking into account ISO TC204 (VRUs, Roadway warning and control systems, active security systems, simulation, and SAE (Data logger, ISO/SAE PAS 22736 Taxonomy AD)
  - SC 31 Data communication,
  - SC 32 Electrical and electronic components and general system aspects,
  - SC 33 Vehicle dynamics and chassis components,
  - SC 35 Lighting and visibility"
  - SC 37 Electrically propelled vehicles,
  - SC 39 Ergonomics

ISO TC22 AG1
Automated driving ad hoc group

ISO TR 4906 Report on standardization prospective for automated vehicles (RoSPAV)

Key future needs, opportunities and recommendations:

- Vehicle systems, reaction of the vehicle (minimum risk manoeuvres) e.g. ISO 23793 Intelligent transport systems — Fallback functions for automated driving systems, under development TC 204, SC33 should be asssociated)
- Human factors:
  - Driver monitoring (TC 22/SC 39 already published ISO/TR 21959-1 Human performance and state in the context of automated driving — Part 1: Common underlying concepts),
  - External HMI (users outside vehicle signalling, ODD status visible to outside)
  - internal HMI (TC 22/SC 39 already published ISO/TR 21959-1 Human performance and state in the context of automated driving — Part 1: Common underlying concepts)
- Safety requirements (Perception, Data storage system for AD DSS-AD, specific aspects for Electric Vehicles (SC 37), Validation, Connectivity, Digital mapping systems, Vehicle-infrastructure integration (infrastructure signes)).

ISO TC22 AG1
Automated driving ad hoc group

ISO TR 4906 Report on standardization prospective for automated vehicles (RoSPAV)

Way forward – two recommendations:

RESOLUTION 941 – Follow-up activity for ADAG

- TC22 agreed to create a coordination group, specific to AD projects. This group shall consist of a representative from each concerned SC to ensure the coordination of new projects. TC204 is invited to participate in this group to improve the coordination also between TC22 and TC204. Ideally that coordination group should be co-chaired by one expert from ISO TC22 and one from ISO TC204. ToR for this group shall be provided by SAG of TC22 in conjunction with TC204 before end of September 2019.

RESOLUTION 942 – Coordination of automated driving topics within the ISO community

- ISO TC22 is proposing ISO TMB to create a small and efficient consulting group that should help to avoid overlapping project initiatives within the ISO community. Relying on the knowledge of the experts being active in ISO TC22 and ISO TC204, ISO TC22 recommend ISO TMB to support that consulting initiative. TC22 is offering to overtake the responsibility to manage that initiative, ideally with help of TC204.

ISO DTR 4804/White Paper (12 Principles of AD)

- Safe operation (dealing with **degradation** (performance related), **Fail operational** (limited to safety-related function or component), transfer to safe condition (acceptable risk condition), **sufficient time to transfer** to **operator/driver**
- **Operational design domain** - ODD (Typical situations that can be expected shall be managed; **ODD determination: if system reaches its limits and compensates or issues/requests a handover in sufficient time frame**).
- Vehicle **Operator-initiated Handover** (explicit, high confident intent).
- **Vehicle-initiated Handover** (if failing in time, vehicle must perform a **minimal risk maneuver**; request should be clearly understandable and manageable).
- **User responsibility** (user state monitoring, responsibility of user always clear, driving mode awareness all time).
- **Interdependency** between the **Vehicle Operator** and the **Automated Driving State** (overall evaluation of system safety needs to take effects on the driver due to automation into account, even when they occur immediately after the period of automated driving has ended and when a direct link to the automated driving part of the journey can be drawn).

ISO DTR 4804/White Paper (12 Principles of AD)

- **Safety assessment** (V&V used to ensure that safety goals are met, consistent improvement of overall safety achieved).
- **Security** (Cybersecurity threat protection ensured).
- **Passive safety** (crash scenarios and vehicle layout and automation; **alternative seating and interior** shall not reduce occupant protection).
- **Behaviour in traffic** (applicable traffic rules obeyed by automated vehicle, behaviour easy to understand, predictable and manageable for other road users (VRUs)).
- **Data recording** (record status data for event or incident tracking compliant with privacy laws).
- **Safe layer** (**fail-aware**: system shall recognize its limits, react to minimize risks, if safe transition is not possible).

ISO 4804 requires **7 Failsafe-Capabilities** of an AD Systems to meet 5 **Challenges**:

- Statistical demonstration avoidance of unreasonable risk and positive risk balance
- System safety with driver interaction (especially take-over manoeuvres)
- Consideration of scenarios currently not known
- Validation of various system configurations and variants
- Validation of (sub) systems that are based on Machine Learning

ISO DTR 4804/White Paper
(7 System Fail-safe and 6 Fail-Degraded Capabilities)

- FS_1: Determine location (in relation to its ODD – Operational Design Domain)
- FS_2: Perceive relevant static and dynamic objects
- FS_3: Predict the future behavior of relevant objects
- FS_4: Create a collision-free and lawful driving plan
- FS_5: Correctly execute and actuate the driving plan
- FS_6: Communicate and interact with other road users
- FS_7: Determine if specified nominal performance is not achieved (human factors, misuse, manipulations; deviation from intended functionality, technological limitations, environmental conditions, systematic and random failures)

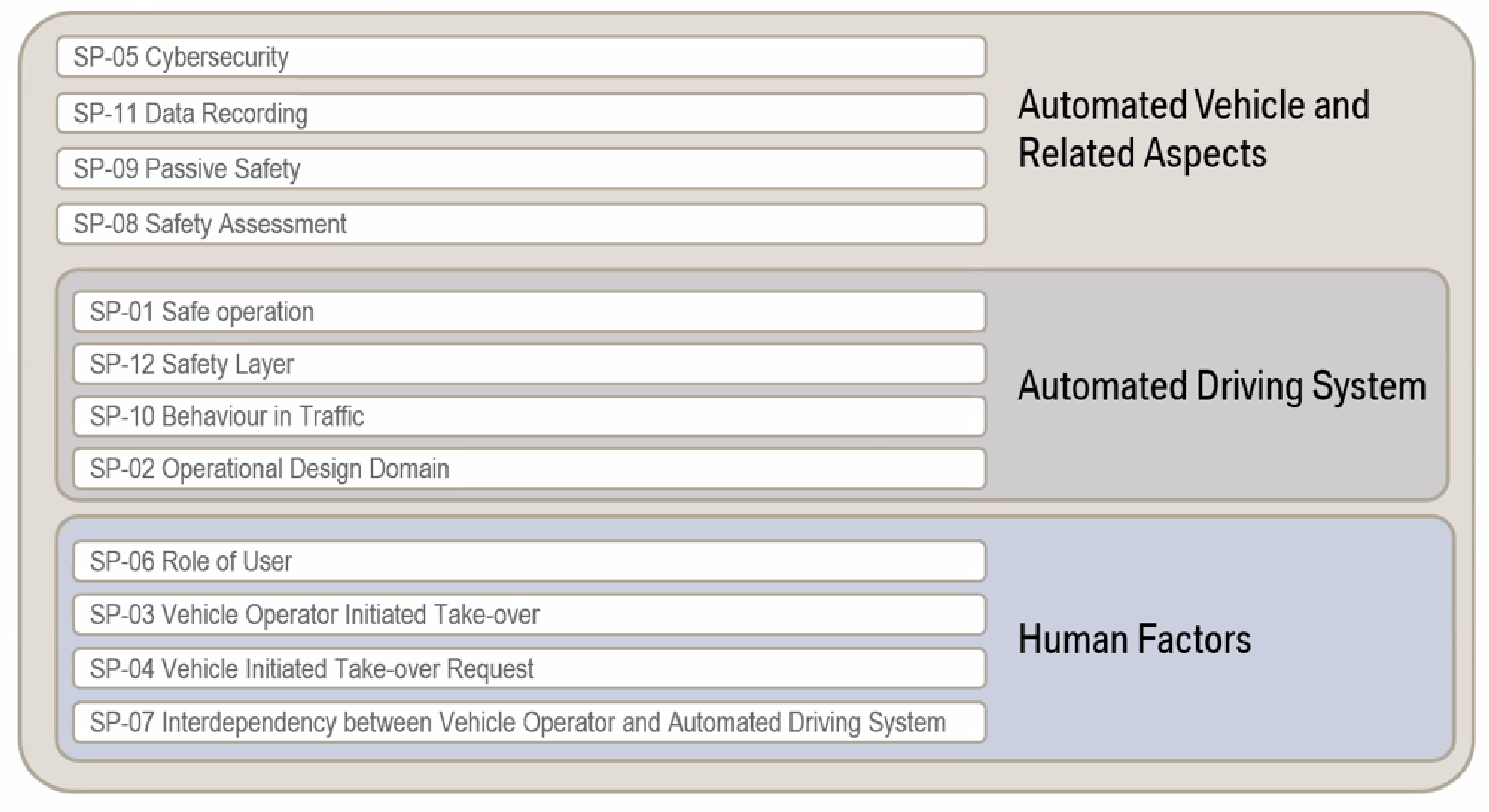
Fail-Degraded Capabilities (Ensure/Detect):

- FD_1: Ensure controllability for the driver
- FD_2: Detect when degradation is not available
- FD_3: Ensure safe mode transitions and awareness
- FD_4: React to insufficient nominal performance and other failures via degradation
- FD_5: Reduce system performance in the presence of failure for the fail-degraded mode (! Has to be defined!)
- FD_6: Perform ODD functional adaptation within reduced system constraints

Are mapped to the 12 Principles for Safety and Cybersecurity for AD!

ISO DTR 4804/White Paper (12 Principles of AD)

Structure after the commenting phase (last week of May 2020, Release July 2nd, 2020).



SP-05 Cybersecurity

SP-11 Data Recording

SP-09 Passive Safety

SP-08 Safety Assessment

Automated Vehicle and Related Aspects

SP-01 Safe operation

SP-12 Safety Layer

SP-10 Behaviour in Traffic

SP-02 Operational Design Domain

Automated Driving System

SP-06 Role of User

SP-03 Vehicle Operator Initiated Take-over

SP-04 Vehicle Initiated Take-over Request

SP-07 Interdependency between Vehicle Operator and Automated Driving System

Human Factors

Close relation to Ethical Aspects/End-User/Public Acceptance of Ethics Guideline for AD

Trustworthiness – a key Public Demand for Acceptance

"Safety first" is no longer sufficient – AD implies "Fail operational", i.e. "smart CPS", i.e. AI and Algorithms

Trust: degree to which a user or other stakeholder has confidence that a product or system will behave as intended (*ISO/IEC 25010:2011(en) Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models (= reliable and dependable))*

ISO/IEC JTC1 AG7 Trustworthiness Definition (July 2019, source AG7

"Trustworthiness, corresponds to the ability to meet stakeholders expectations in a verifiable way".

- Depending on the context or sector, and also on the specific product or service, data, and technology used, different characteristics apply and need verification to ensure stakeholders expectations are met.
- **Characteristics of trustworthiness include, e.g. reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, usability.**

Trustworthiness – a key Public Demand for Acceptance

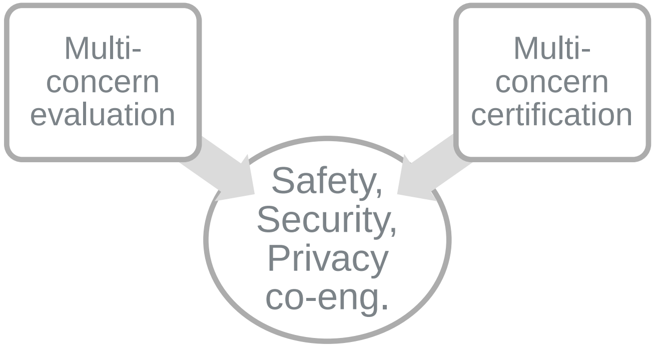
“Safety first” is no longer sufficient – AD implies “Fail operational”, i.e. “smart CPS”, i.e. AI and Algorithms

- Trustworthiness is an attribute that can be applied to services, products,technology, data and information, and in the context of governance, to organizations.
- Trustworthiness is ensured and maintained through
  - sound governance framework and
  - systems engineering practices.

- **Trustworthiness** contributes to the building of **confidence** (in the end, to end-user/public acceptance).

- → **Multi-concern Assurance Cases, more than Safety Case**

SECREDAS and AUTODRIVE standardization activities and interests



Multi-concern evaluation

Multi-concern certification

Safety, Security, Privacy co-eng.

- Safety, security and privacy co-engineering for critical systems, particularly in the basic functional safety standards (IEC 61508-3, IEC 63069, ISO PDTR 27550 - Privacy Engineering, ISO 26262, ISO 21448) – Goals: Fail aware, fail operational, fail degraded
- UNECE regulations, Threat catalogue used
- Automotive Cybersecurity standardization: ISO 21434, ISO PAS 5112, ISO NP 24089 (SW Update-OTA)
- Automated Driving: ISO TR 4609, ISO TR 4804
- Monitor ISO/IEC JTC1 SC41 (IoT), SC42 (AI – Trustworthiness) and SC38 (Cloud computing), IETF and ETSI IoT (AIOTI) on relevant issues for SECREDAS and AUTODRIVE
- ITS Standards: ETSI TC ITS, CEN TC 278, ISO TC 204 → co-operative ITS, e.g. ISO 21217:2014 under review (ITS station units - CALM architecture).

Cooperative ITS

- Detailed discussions in SECREDAS
  - Major committees:
    - ISO TC204 – Intelligent transport systems (ISO TC 268 Green cities,
    - CEN TC 278 - Intelligent transport systems (WG17 Urban ITS, WG16 Coop. ITS)
    - ETSI TC ITS – (Automotive) Intelligent transport systems, IEEE Comm. Stds.
  - Most relevant standardization groups:
    - ISO/TC 204/WG 1 – Architecture.
    - ISO/TC 204/WG 16 – Communications.
    - ISO/TC 204/WG 17 - Nomadic Devices in ITS Systems.
    - ISO/TC 204/WG 18 - Cooperative systems.
    - ISO/TC 204/WG 19 - Mobility integration.

Cooperative ITS

- ITS Services requiring Security (from SECREDAS):
  - Real-time access to time critical vehicle data (collision avoidance, emergency brake, …).
  - Real-time data exchange for road traffic management (green wave information, priority lane access management, interactive optimum vehicle settings to minimize fuel consumption, …).
  - Protection of personal data in compliance with the European "General Data Protection Regulation" (GDPR).
  - Service, repair and maintenance of electronic components of the vehicle.
  - Semi-automated or automated driving (regulated speed, platooning, remote driving…).
  - Remote management of ITS station and software update.
  - Value added services (electric charging, parking.

SECREDAS Standardization Strategy

OUTLOOK: Next steps for Year 3 and Beyond

- Singular achievements as by now are of course worth to be considered, but -

  a discussion within the members working in ISO TC22 Subcommittees („Road vehicles“) and in ITS-related standardization revealed a need for harmonization and joint activities sharing as a common goal:

  - **Bridging the gap** between **ISO TC22/Extended Vehicle standardization** and ITS (secure vehicle interface and gateway) (medium term), meeting needs of both communities
  - **Holistic view at (highly) automated driving (connected/extended vehicles, SotiF related issues, Roadmap Report** on standardization prospective for automated vehicles (RoSPAV), ISO TR 4804 etc.) (mid- to long-term)

  - **Next tasks:** Identifying:
    - Joint forces in a common approach to the various standardization committees we are active already
    - Function blocks from SECREDAS that could be provided towards the end of SECREDAS
  - **Risks:** Remaining time too short for tangible results → At least initiating medium-to-long term tasks!

AIT Austrian Institute of Technology

Acknowledgement

Part of the work presented in the workshop received funding from the EC (ARTEMIS/ECSEL Joint Undertaking) and the partners National Funding Authorities ("tri-partite") through the projects AutoDrive (737469), and SECREDAS (783119) (in Austria the Austrian Federal Research Promotion Agency (FFG) on behalf of the Federal Ministry of Climate Action, Environment, Mobility, Innovation and Technology (BMK)).

Erwin Schoitsch - Erwin.schoitsch@ait.ac.at

Thank You for Your Kind Attention !

S

- a