Ongoing Cybersecurity and Safety Standardization Activities Related to Highly Automated/Autonomous Vehicles

Erwin Schoitsch(✉) and Christoph Schmittner

AIT Austrian Institute of Technology GmbH, Giefinggasse 4, 1220 Vienna, Austria
{erwin.schoitsch,christoph.schmittner}@ait.ac.at

Abstract. Highly automated/autonomous vehicles using extended features like Vehicle to Vehicle (V2V) or Vehicle to Infrastructure (V2I), cognitive systems for decision taking, needing extensive perception features and sophisticated sensor functions, cause a considerable shift in safety and cybersecurity (trustworthiness) co-engineering and assurance. To achieve trust of the public/users, standards and certification/qualification are challenged, not comparable to conventional "singular vehicle only" issues. The paper highlights the necessary evolution in the automotive and related standardization landscape, including ethics guidelines and recent activities, and the consequences from upcoming UNECE (United Nations Economic Commission for Europe) regulations. An Overview on ongoing work in large European ECSEL projects, SECREDAS and AutoDrive, including standardization, is provided.

Keywords: Automated driving · Autonomous vehicles · Functional safety · Cybersecurity · Standardization · Trustworthiness · Ethics guidelines · SotiF (Safety of the intended Functionality) · Ethics guidelines

1 Introduction

Autonomous vehicles and even assistive features of highly automated vehicles area causing a shift in the basic control paradigm of vehicles. In the past, the main task of vehicle systems was to capture the driver's control command and transmit it to the actuators without misinterpretation. The main focus was functional safety, e.g. the protection against failures in the electronic, electric and programmable electric systems (E/E/PE) related to this task. This was addressed in ISO 26262 [1], a domain specific adaption of the generic functional safety standard IEC 61508 [2]. The first version was published in 2011, the second version in 2018.

With the change towards assistive features, the role of the E/E/PE-systems also changed towards an optimization of driver's control command and even autonomous decision making. While increasing driving efficiency and road safety, the potential for adverse effects are also increasing. Manipulated E/E/PE systems are no longer restricted to an incorrect reaction to driver's control command but can also trigger completely new actions. In a similar way, systems, which perceive and react on their environment to

C. Zachäus and G. Meyer (Eds.): AMAA 2020, LNMOB, pp. 72–86, 2021.
https://doi.org/10.1007/978-3-030-65871-7_6

optimize actions or take decisions, need a certain level of guarantee that the perceived environment represents the real environment.

The automotive industry and research field reacted on these new challenges and developed methods and approaches, which resulted in standards, collecting the best practice and industrial accepted and proven engineering processes.

Noteworthy results are ISO PAS 21448 “Road vehicles—Safety of the intended functionality” [3] which focuses on novel parts of safety aspects beyond nominal performance, as introduced by automated and autonomous vehicles, and ISO/SAE DIS 21434 “Road vehicles—Cybersecurity engineering” [4], a joint effort by ISO and SAE to standardize automotive cybersecurity engineering.

In the following chapter, we will present an overview about ongoing developments towards highly automated and autonomous vehicle systems and their impact on society. This will be followed by an overview about automotive standardization, status and content. Finally, we will conclude with an overview about the SECREDAS and AutoDrive research projects referencing some key results, and the activities in addressing novel automotive challenges.

2 Automotive Standardization Activities

2.1 Automotive Standardization Landscape

There does exist a huge landscape of automotive standards with respect to electric, electronic and programmable electronic (E/E/PE) systems. Most are covered by ISO TC22, “Road vehicles”, and the associated subgroups. Other areas relevant for highly automated/autonomous systems are covered e.g. for ITS (Intelligent Transport Systems) in ETSI and ISO TC 204, or by ISO/IEC JTC1 for IoT (Internet of ThingsSC41) and Artificial Intelligence (ISO/IEC JTC1 SC42), particularly concerning trustworthiness of such systems (technically, but also from the ethics viewpoint) (see Fig. 1).

We focus here on standardization for dependability. Dependability summarizes the ability of a system to be trusted by its users, e.g. to perform its mission as intended. This notion was introduced in [5], and the different dependability attributes, threats and means were introduced:

- Safety and security requirements can be incompatible.
- Requirements can be derived from the other domain (safety requirements, which cause a security requirement and vice versa).

Historically, a major focus of the automotive domain was on functional safety as the subset of safety which was focused on risks due to failures in the E/E/PE-systems (ISO 26262 [1]). Due to the rising number and complexity of sensors, communication and decision taking systems, and the increasing security risks endangering safety, this was extended to include automotive cybersecurity and safety of the intended functionality (SotiF) [3].

Figure 2 gives a view on these attributes. Important are the cross-relations between all these attributes. One of the first systematic analysis of this has been done in [6], identifying the following relations:

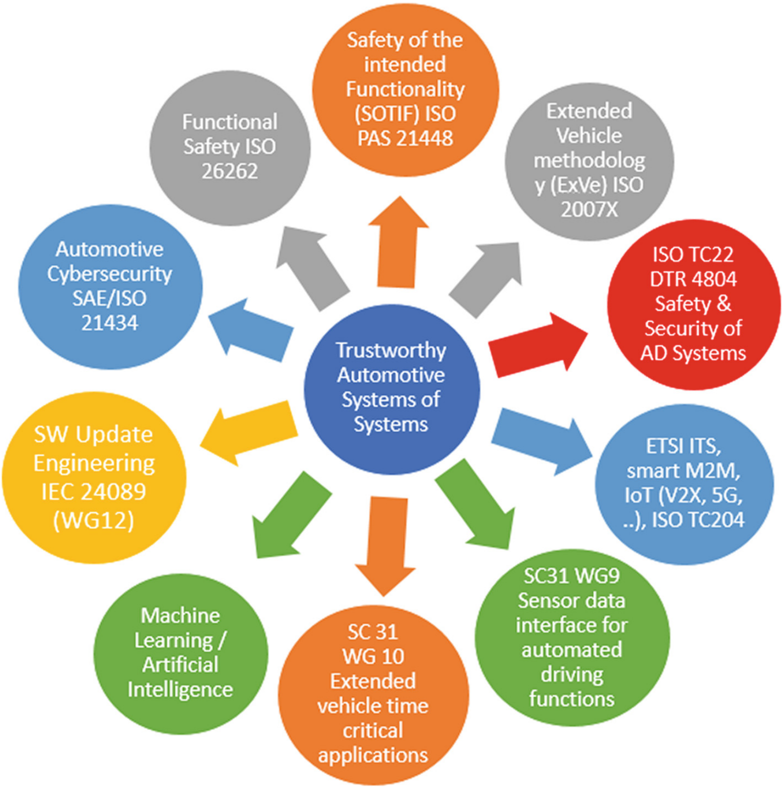

Safety of the intended Functionality (SOTIF) ISO PAS 21448
Functional Safety ISO 26262
Extended Vehicle methodolog y (ExVe) ISO 2007X
Automotive Cybersecurity SAE/ISO 21434
ISO TC22 DTR 4804 Safety & Security of AD Systems
Trustworthy Automotive Systems of Systems
SW Update Engineering IEC 24089 (WG12)
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

Fig. 1. Standardization landscape for (highly automated) automotive systems

- Requirements can be incompatible
- Requirements can be derived from the other domain (safety requirements which causes a security requirement)

In order to identify these interdependencies a conflict resolution and integration of requirements was proposed in [6].

Based on this, newer standards (one of the additions in the 2018 version of ISO 26262 [1], compared with the 2011 version) required communication channels for such interactions between different dependability related disciplines. The approach in the automotive domain was to require such communication channels and give guidance from the respective standard towards other domains. As an example, ISO 26262:2018 requires communication channels and contains guidance on the interaction from functional safety towards cybersecurity (particularly in Part 2 and Annex F of Part 2).

2.2 Safety of the Intended Functionality

The SotiF process [3] is based on ISO 26262 [1] and it is assumed that the lifecycle is enhanced with additional activities to ensure that the likelihood of a hazardous event is

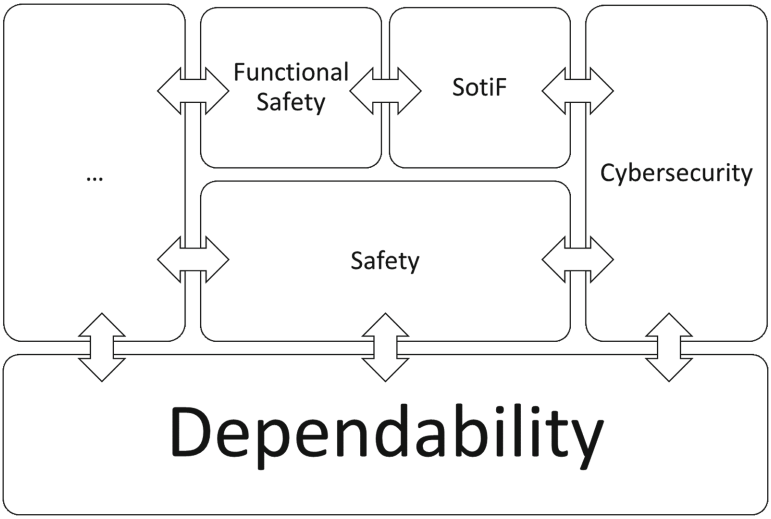


Fig. 2. Automotive dependability with the focus on safety and cybersecurity

sufficiently low. The assumption is, that, compared to ISO 26262, which scope does not include nominal performance issues, a certain amount of unsafe behavior is not known, (e.g. of sensors and their intended functionality which may not be sufficiently known).

Figure 3 gives an overview of the concept and approach of SotiF. This is based on the assumption that, compared to functional safety, not all situations are known for SotiF, since SotiF is based on a perception and reaction of the real world.

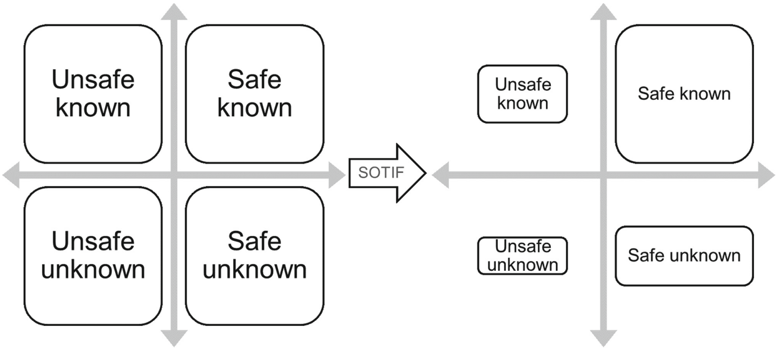


Fig. 3. Overview of the SotiF approach

The goal is therefore not only a reduction of the risks of known hazards to a tolerable level but also a reduction of the unknown. Examples for this are the difficulties Volvo's self-driving cars had with the detection of kangaroos [12]. This was based on the different manner of movement (e.g. hopping) compared with other, and especially with native large animals from Sweden. This reduction of unknowns includes also a learning of the engineers about the later application environment to understand potential difficult scenarios and situations.

Based on this a test and verification plan can ensure that the vehicle has a sufficient rate of “safe” reaction, even on difficult scenarios and under problematic circumstances. This is supplemented by real world evaluation of the system. UL4600 was especially developed for testing and evaluation [13]. This document describes an approach to ensure safe self-driving cars based on an extended safety-case and with a focus on highly-automated and edge-case analysis [14].

Nevertheless, the topic on how to ensure sufficient testing and assurance is still not completely addressed. A sufficient combination of “testing in the loop” (based on simulation, safe, cheap but only pre-defined scenarios), “testing in controlled environments” (test-tracks, safe but environment does not contain surprises) and “real world testing” (safety risks, costly) needs research.

2.3 Automotive Cybersecurity and UNECE Draft Regulation

The first official guideline regarding automotive cybersecurity was SAE J3061 [7]. This document was intended as a first step, collecting engineering methods and approaches, which could be applicable to the automotive domain. This was not an international standard, but a first step as guidebook. Work with this guidebook demonstrated applicable methods, but also still existing gaps [8, 9].

Based on this, ISO and SAE decided to cooperate on the development of an international standard regarding automotive cybersecurity engineering. Here an additional driver of this development was the parallel development of a new UNECE draft regulation [24] regarding cybersecurity for the type approval. Currently the draft international standard (ISO/DIS 21434) was published and the publication of the international standard (IS) is planned for end of 2020.

The standard offers requirements and guidance on four topics. Processes for cybersecurity on organizational and project level define a framework for cybersecurity engineering and the integration of cybersecurity with other disciplines. This is followed by an automotive specific approach towards risk management, based on the generic risk management approach from ISO 31000. The last two parts are on cybersecurity engineering, including production, and post-production with a focus on maintaining cybersecurity of the system.

2.4 Software Update (Over the Air) and UNECE Draft Regulation

Similar to the topic of cybersecurity, UNECE developed a draft regulation on software update [25]. This time standardization lagged behind and the standardization process started after the draft regulation was available. The focus of the draft regulation is on requirements for the update system in vehicle and backend and on organizational processes. The goal is to a) ensure updates while mitigating safety, security and other risks and b) controlling the versions of software on a vehicle for regulatory processes.

Since regulatory requirements are on a very high level there was a need to collect the interpretation and state of the art. For this a standardization project was started last year, which will develop a standard on software update engineering (ISO 24089). Here we have also a strong linkage between technical work and standardization. The topic of fail-safe/fail-tolerant update systems is important for the overall AutoDrive objective of fail-safe/fail operational automated vehicles, and security topics are the main focus of SECREDAS. There is a overarching activity with multiple project partners to develop an implementation of "IEEE-ISO 6100.1.0.0 Uptane Standard for Design and Implementation".

Besides implementing the standard on a relevant environment to demonstrate the technology, an additional goal is to extend the focus from secure updates towards safe updates. This includes an update framework which

- ensures before the update that the vehicle is in a status where an update is possible (vehicle state, usage of systems, available energy, consent from vehicle user),
- controls and restricts vehicle operations during the update in order to avoid undefined situations (usage of a half-updated ECU),
- and ensures safe operation after the update (self-tests and monitoring, inform the vehicle user about success/failure and changed features)

The main challenge here with a remote update, compared to an update during regular maintenance is the unreliable connection, missing trained staff and restricted control about the vehicle environment and state.

2.5 Ethics Guidelines and Rules for Autonomous Driving

Several organizations from standardization, governmental advisory groups, professional and scientific associations have already produced guidelines and recommendations on how ethical principles should be considered in taking up new technologies, particular when applying cognitive systems in automation (not only automotive for highly automated/autonomous driving).

A few examples (not exhaustive) are [10, 11]:

- Informatics Europe and ACM Europe [18] "When Computers Decide"
- The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems (AI/AS) (April 2016)
    - Ethically Aligned Design: A Vision for prioritizing human wellbeing with artificial intelligence and autonomous systems
    - Identification and recommendation of ideas for standards projects focused on prioritizing ethical considerations in AI/AS.
    - IEEE ECAIS "Ethics Certification for Autonomous and Intelligent Systems" (Industry Connections Activity Initiation Sept. 2018).
- IEC/SMB Ad-hoc group on autonomous systems and ethics (AHG 79), recommendation "*…assessing the role of IEC and standards in addressing ethics, trust and values particularly in autonomous systems, and making recommendations. The review should consider the work of JTC 1/SC 42 (Artificial Intelligence), ACART (Advisory*

Committee on Applications of Robot Technology), ACOS (Advisory Committee on Safety), TC 59 (Performance of household and similar electrical appliances), TC 100 (Audio, video and multimedia systems and equipment), SyC AAL (Systems Committee on Active Assisted Living), SyC Smart Cities, IEEE, ISO etc."

- ISO/IEC JTC1 SC42 (Artificial Intelligence): Technical Management Board resolution 53/2018: *Approval of the inclusion of certain aspects of 'societal concerns' in the ISO/IEC JTC1/SC 42 programme of work.*
- ISO TC241 Road Traffic Safety (RTS) – new work item under discussion: "Ethical considerations for driverless vehicles" (IEC 39003), which had to be redrafted because of criticism from other automotive-related TCs (e.g. TC22).
- EC: "Ethics Guidelines for Trustworthy AI" [19]
- German Federal Ministry of Transport and Digital Infrastructure (June 2017), "Ethics Commission – Automated and Connected Driving" [20]

The document of the German Ethics Commission for Automated and Connected Driving defined 20 principles to follow for an ethical and human-centered approach to approve autonomous vehicles. This ethics commission was the first of its kind and the approach was the initiator for the EC to start their ethics task force, leading to high level structural dialogues under German leadership, with members (according to the report of June 2018) Germany (Chair), Austria, Luxembourg, United Kingdom, European Commission, ACEA, CLEPA (automotive associations). The report is available (see [19]). Most principles are also reflected in the draft discussions to ISO DTR 4804 ([16], derived from [15]) and the NHTSA (National Highway Traffic Safety Administration, US) (shortened):

- The primary purpose of partly and fully automated transport systems is to improve safety for all road users, to increase mobility opportunities and to make further benefits possible. To preserve personal autonomy, which means that individuals enjoy freedom of action, is another principle
- The protection of individuals takes precedence over all other utilitarian considerations. The licensing of automated systems is only justifiable in case of a positive balance of risks.
- The public sector is responsible for guaranteeing the safety of the automated and connected systems introduced and licensed in the public street environment. Driving systems thus need official licensing and monitoring.
- The personal responsibility of individuals for taking decisions is an expression of a society centered on individual human beings, with their entitlement to personal development and their need for protection.
- Automated and connected technology should prevent accidents wherever this is practically possible. This includes dilemma situations, where they have to drive in a defensive and anticipatory manner, posing as little risk as possible to vulnerable road users.
- A statutorily imposed obligation to use fully automated transport systems or the causation of practical inescapabilty is ethically questionable.

- In unavoidable hazardous situations, the protection of human life enjoys top priority in a balancing of legally protected interests, e.g. to accept damage to animals or property in a conflict.
- Genuine dilemmatic decisions, such as a decision between one human life and another, depend on the actual specific situation, and cannot be clearly standardized, nor can they be programmed such that they are ethically unquestionable. It would be desirable for an independent public-sector agency (e.g. a Federal Office for Safety in Automated and Connected Transport) to systematically process the lessons learned.
- In the event of unavoidable accident situations, any distinction based on personal features (age, gender, physical or mental constitution) is strictly prohibited. It is also prohibited to offset victims against one another. General programming to reduce the number of personal injuries may be justifiable. Those parties involved in the generation of mobility risks must not sacrifice non-involved parties.
- In the case of AD systems, the accountability shifts from the motorist to the manufacturers and operators and to the bodies responsible for taking infrastructure, policy and legal decisions.
- Liability for damage caused by activated automated driving systems is governed by the same principles as in other product liability.
- The public is entitled to be informed about new technologies and their deployment in a sufficiently differentiated manner.
- The complete connectivity and central control of all motor vehicles within a digital transport infrastructure is ethically questionable.
- Automated driving is justifiable only to the extent to which conceivable cybersecurity attacks do not result in such harm as to lastingly shatter people’s confidence in road transport.
- Autonomy and data sovereignty of road users: The vehicle keepers and vehicle users decide whether their vehicle data that are generated are to be forwarded and used.
- No abrupt handover of control to the driver (“emergency”): To enable efficient, secure human-machine communication and prevent overload, the systems must adapt to human communicative behaviour.
- It must be possible to clearly distinguish whether a driverless system is being used or whether a driver retains accountability with the option of overruling the system. This applies especially to the human-to-technology handover procedures.
- In emergency situations, the vehicle must autonomously, i.e. without human assistance, enter into a “safe condition”. Harmonization, especially of the definition of a safe condition or of the handover routines, is desirable (standardization).
- Learning systems that are self-learning in vehicle operation and their connection to central scenario databases may be ethically allowed if they generate safety gains. Self-learning systems must not be deployed unless they do not undermine the safety requirements. It is advisable to hand over relevant scenarios to a central scenario catalogue at a neutral body in order to develop appropriate universal standards, including tests.
- The proper handling of automated driving systems should be taught appropriately during driving tuition and tested (part of general education).

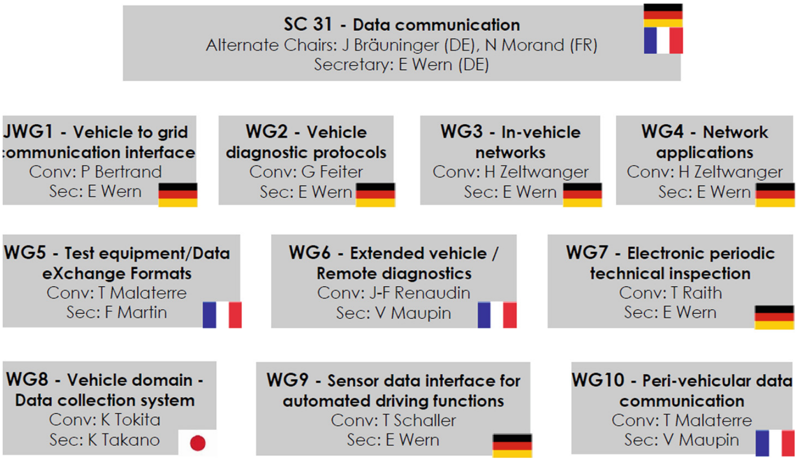
In “My agenda for Europe” [21] of Ursula von der Leyen, the President of the European Commission, one chapter is dedicated to “A Europe fit for the digital age”.

It focuses on AI, IoT, 5G, and ethical and human implications of these technologies, empowering people through education and skills, and protecting ourselves with respect to the risks of these technologies. This is a strong indication, that efforts to considering ethical aspects in time will be continued.

3 Standardization Towards Autonomous Vehicles

The increased use of automated support functions (ADAS, Advanced driver assistance systems) led to an substantial increase in standardization in related areas for road vehicles (ISO TC22, TC 204 Intelligent transport systems, TC 241 Road safety, each with many subcommittees – some evolving standards do already contain a phrase like “for automated driving (functions)”), and other standardization groups like SAE (US), ETSI ITS, CEN/CENELEC, and UNECE WP.29 (UN Economic Commission for Europe, who sets the regulatory framework valid in most countries of the world).

Looking at the structure of ISO TC22 SC31 (Fig. 4) indicates already, that some topics concern automated driving functions, but outside SC32, e.g. WG6, WG9 and WG10, but there are also overlaps with other subcommittees (e.g. JWG1 with SC37, electrically propelled vehicles, and also with SC32 WG 12, Software update and ExVe functions, if communication is done over the air).



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

Fig. 4. Structure of ISO TC2 SC31 – AD-relevant WGs (WG6, WG9, WG10) (source: ISO TC22 SC31 report to TC22 ADAG on Automated Driving, 2018)

Being aware of the risk that competing standards in particular (sub-)areas might arise, ISO TC22 SAG (Strategic Advisory Group) initiated AG1, an Ad-hoc group for automated driving (ADAG) for a mid-term roadmap task in this field. This resulted in a report ISO/CD TR 4609 “Road vehicles – Report on standardization prospective for automated vehicles (RoSPAV)” [23]. It provides an overview over all relevant standards from ISO TC22 SC 32 (Electrical and electronic components and general aspects), SC31

(Data communications, including Sensor data interface for automated driving functions, Extended vehicle (ExVe) and ExVeS time-critical applications), SC33 (Vehicle dynamics and chassis components), SC 39 (Ergonomics), SC37 (Electrically propelled vehicles), and TC204 (ITS) WG 14 (Total system functionality and behavior).

Additionally, the report provides an outlook on future needs, opportunities and recommendations for standardization. These recommendations will be considered (e.g. by the authors working in EU-research initiatives and projects (ECSEL, Horizon)) in context of the standardization objectives of these work programs.

Key issues identified are concerning (addressed also in the ethics guidelines):

- Driver monitoring systems (define globally addressed metrics).
- Internal HMI (particularly for take-over, drivers' inactivity, on/off s, urgency buttons, maneuvers information, police orders, …).
- Reaction of the car (minimal risk conditions, fail operational or degraded, environmental conditions, communication with VRUs).
- Perception (common requirements for assessment of sensor functionality, independent of technology, quantification of performance and other dependability/trustworthiness attributes)
- Infrastructure signs (worldwide standard for design for perception)
- Connectivity (for cooperative intelligent transport systems, interoperability V2V, V2I (complementary to ETSI, ITU, SAE, TC204).
- Digital mapping system (reliable geolocation, interoperable platforms)
- Data storage system for AD (DSS-AD) (Event data recorder, plus DSSAD complementarity)
- Specific aspects for electrical vehicles (EV) (electrical safety, etc.)
- Validation (SotiF, validation based on test scenarios (SC33/WG9))

A key document for future standardization for automated driving is the "White Paper" [15]. This document provides an extensive overview over all relevant state-of-the-art safety by design, validation and verification methods, focusing on the challenges of automated/autonomous driving. The goal is to ensure the requirement of all existing ethical and technical guidelines to achieve a "positive risk balance", as compared with the situation of human driving. It takes into account the existing road vehicle standards, precision maps and navigation standards (ISO19157:2013, ISO/TS 16949:2009), and system and software engineering standards (ISO/IEC/IEEE 15288:2015). Cybersecurity and required capabilities of automated driving are described in detail as well as their elements (technologies and rules) for implementation. The document is positioned around the "Twelve Principles of Automated Driving" as a baseline for safe automated driving:

- Safe operation (dealing with degradation (performance related), Fail operational (limited to safety-related function or component).
- Vehicle operator-initiated handover (explicit, high confident intent).
- Operational design domain (typical situations that can be expected shall be managed; odd determination: system reaches its limits and compensates or issues/requests a handover in a sufficient time frame).

- Security (cybersecurity threat protection ensured).
- User responsibility (user state monitoring, responsibility of user always clear, driving mode awareness all time).
- Vehicle-initiated handover (if failing in time, vehicle must perform a minimal risk maneuver; request should be clearly understandable and manageable).
- Safety assessment (V&V used to ensure that safety goals are met, consistent improvement of overall safety achieved).
- Passive safety (crash scenarios and vehicle layout and automation; alternative seating and interior shall not reduce occupant protection).
- Data recording (record status data for event or incident tracking compliant with privacy laws).
- Behavior in traffic (applicable traffic rules obeyed by automated vehicle, behavior easy to understand, predictable and manageable for other road users (VRUs)).
- Safe layer (the system shall recognize its limits, and react to minimize risks, particularly if safe transition is not possible).

Most of these conditions fit well also to the ethical rules, which address the user and public acceptance issues.

This document is now the basis for the evolving standard ISO TR 4804 [16], "Road vehicles – Safety and security for automated driving systems – Design, verification and validation methods" (a technical report). The kick-off meeting was February 19–21, 2020, in Paris, the author took part in the discussions. The working document follows the white paper, the parts on motivation and general challenges, was removed because these parts are not required in a standard. Details on some technologies and issues handled already in existing standards are either shortened (with references) or put into an informative annex (e.g. use cases as examples). There were extensive discussions on terms and definitions, which is crucial, because important clauses refer to them and common understanding is required (e.g. "fail degraded" will be used, "fail operational" was removed, the issue of performance has to be separated between planned performance degradation because of bad weather conditions, or degradation because of failure or uncertain decision situation). The DTR 4804 will be soon distributed for comments to the national committees, taking into account the results of the Paris meeting.

4 Ongoing Research and Conclusions

Effective work is done in many European and national projects. Two examples are the ECSEL JU projects SECREDAS (grant agreement 783119-2, started 2018, https://secredas.eu/) and AutoDrive (grant agreement 78119-2, started 2017, https://autodrive-project.eu/). AutoDrive is the corner-stone project of the ECSEL Lighthouse cluster "Mobility.E" (https://www.ecsel.eu/mobilitye), SECREDAS is also a partner project in Mobility.E.

SECREDAS stands for "Product Security for Cross Domain Reliable Dependable Automated Systems". The high-level goal of SECREDAS is to develop and validate multi-domain architecting methodologies, reference architectures and components for autonomous systems, combining high security and privacy protection while preserving functional-safety and operational performance. This should increase consumer trust in connected and automated transportation (major focus automotive, but also railways), and in medical industries.

SECREDAS will be making a first important step into the direction of developing "trust"-building components and (sub-)systems for the European industries of tomorrow. Four main directions are taken: Reference Architecture, Powerful Components, Common Approaches, Scenarios & Pilot Tests.

The approach taken is to study a number of relevant use cases with specific requirements of safety, security, and privacy. Together with current state-of-the-art reference architectures, the use cases will lead to a next generation of reference architecture and common elements for multiple application domains. On top of that, several domain-specific solutions will be built to work out domain-specific and common demonstrators for the different application domains.

In SECREDAS, a number of relevant user scenarios with specific requirements of safety, security and privacy are studied in detail. A set of "Common technology elements" for achieving the overall goal of safe and secure automated systems was defined. Vehicle sensing, vehicle connectivity (particularly addressing ITS standards mentioned before), and in-vehicle networking are the key "abilities" for safe and secure automated systems. Demonstrators are foreseen for health, rail and "common demonstrators" (automotive). Standardization, qualification and certification is an important work package in SECREDAS. Particularly the new evolving standard ISO 4804 on "Road vehicles – Safety and cybersecurity for automated driving 4 systems – Design, verification and validation methods" should benefit from SECREDAS work. The outcomes of the work (technologies and use cases) are taken over for contribution to standardization by partners, who are members of standardization groups. The authors themselves are involved and leading this work package. The result of the first standardization deliverable, a survey on the applicability of safety, security and privacy standards in the three domains (with most contributions from the automotive sector) was published in a paper at the DECSoS Workshop at Safecomp 2019 [22], considering additionally the needs and reasons for certification according to these standards. The key result of this work were the answers to the following research questions (RQ1 – RQ4):

- RQ1. What standards are applicable and is there any difference between the availability of safety, security and privacy standards?
  "Safety standards for specific industrial sectors are available, as specializations of one basic standard IEC 61508 [2]. Security standards with different origins address different themes, while few are targeted to specific industrial sectors. There are fewer privacy standards than for safety/security, and there is no privacy standard targeted to specific sectors."
- RQ2. How are the Sa/Se/Pr (Safety/security/Privacy) standards practiced?
  "ISO 2700X and ISO 15408 are the most applied standards among all the studied standards. The application of safety standards is significantly more often imposed by customers and regulators than that of security/privacy standards. The conformance to safety standards is slightly more rigorously evaluated than that of security/privacy standards."

- RQ3. Which methodologies are applied for Safety/Security/Privacy evaluation? - *"Among safety analysis methodologies, FMEA [6], FTA [7] and HARA (Hazard Analysis and Risk Assessment) [8] are commonly used. Security analysis methodologies most commonly used are STRIDE [9] and Common Criteria [10]. The usage of security analysis methodologies is less convergent than of safety ones."*
- RQ4. Which tools are employed in Sa/Se/Pr engineering?
  MathWorks Simulink and IBM Rational DOORS kit are more used for safety and security engineering than the other tools. On privacy engineering, only very few tools are available and applied in practices.

The SECREDAS survey reveals as a result that security/privacy standards are gaining popularity in safety-critical industrial sectors, though both their development and their practices are less mature than that of safety standards. Standards linking safety and security engineering are not widely used, indicating that a multi-concern point of view for Sa/Se/Pr co-engineering is not yet widely adopted.

AutoDrive stands for "Advancing fail-aware, fail-safe, and fail-operational electronic components, systems, and architectures for highly and fully automated driving to make future mobility safer, more efficient, affordable, and end-user acceptable". The project is centred around the key attributes "fail safe", "fail aware", and "fail operational" of autonomous systems in the automotive and aircraft domain. The project is organized around so-called 10 supply chains, which are

- SC1: Fully automated driving (AD) and flying systems (bus, electrically propelled aircraft) targeting SAE level 5.
- SC2: Highly automated driving (SAE level 4; driver/system transition, V2V and V2I, dynamic planning)
- SC3: Cooperative active safety for AD (fail-operational collision avoidance, connectivity, critical situation handling)
- SC4: Fail-operational 800 V automotive powertrain
- SC5: Safe, secure and low latency communication
- SC6: Acquisition, 360° sensing, perception, environmental awareness
- SC7: Embedded intelligence (reasoning, decisioning, planning and controlling) and systems for AD
- SC8: Fail aware systems and components health prediction (weakness aware systems)
- SC9: End-user acceptance, certification and standardization of AD systems (includes societal and ethical aspects as described before)
- SC10: Impact on vehicle and road safety (Vision zero)

SC4–SC8 are the "technology enablers", the core of the research. The results are validated in the "output enablers" SC1–SC3. SC9 and 10 are reflecting the economic, societal and European impact.

One quasi-standards related key result was the computer vision benchmark WildDash https://wilddash.cc/ [26], which was incepted in the project. It enables better comparison of computer vision algorithms and, in the future, will help in certifying computer vision based automotive components. It is a key element to verify and validate "fail operational" behavior of autonomous systems, a key target of AutoDrive. The approach of an algebraic framework for runtime verification can be used to do predictive monitoring and detecting trends in a system. Early detection of upcoming problems is an enabler to build fail operational systems, because counter measures can be taken before the actual fault hits. The application to AutoDrive use cases is presented in a paper for Safecomp 2020 "Weakness monitors for fail aware systems" [27].

Several partners play an important role in standardization in ISO TC22 committees, particularly in the field of safety, cybersecurity and the new committee working on ISO DTR 4804, but are also active in ISO/IEC JTC1 SC41 (IoT) and SC42 (Artificial intelligence), with focus on trustworthiness issues for decision taking cognitive systems as the basis for autonomy. Most issues addressed by international standardization to keep pace with the developments in the domain of highly automated/autonomous systems/vehicles are tackled in these projects.

Although many details of the evolving system concepts and the implementations to build trustworthy highly automated/autonomous vehicles, being at the same time ethically and socially beneficial or at least tolerable, are still unclear, the approaches taken by the scientific community are looking promising.

Acknowledgement. Part of the work received funding from the EC from both, the EC ECSEL JU and the partners' national funding authorities (in Austria FFG (Austrian Research Promotion Agency) on behalf of BMK, (Austrian Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology) - (Grant agreements n° 737469-2 (AutoDrive) and n° 783119-2 (SECREDAS)).

References

1. ISO, ISO 26262: Road vehicles - Functional safety. International Standard (2018)
2. IEC, IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. International Standard (2010)
3. ISO, ISO PAS 21448: Road vehicles — Safety of the intended functionality. Publicly Available Specification (2019)
4. ISO, SAE, ISO/SAE DIS 21434: Road vehicles—Cybersecurity engineering. Draft International Standard (2020)
5. Avizienis, A., Laprie, J.-C., Randell, B.: Fundamental concepts of dependability. Computing Science, University of Newcastle upon Tyne (2001)
6. Eames, D.P., Moffett, J.: The integration of safety and security requirements. In: International Conference on Computer Safety, Reliability, and Security. Springer, Heidelberg (1999)
7. SAE, Society of Automotive Engineers: SAE J3061-cybersecurity guidebook for cyber-physical automotive systems (2016)
8. Schmittner, C., et al.: Using SAE J3061 for automotive security requirement engineering. In: International Conference on Computer Safety, Reliability, and Security. Springer (2016)
9. Macher, G., et al.: A review of threat analysis and risk assessment methods in the automotive context. In: International Conference on Computer Safety, Reliability, and Security. Springer, Cham (2016)
10. Schoitsch, E.: Smart Systems Everywhere – Intelligence, Autonomy, Technology and Society. In: IDIMT 2018, Proceedings, pp. 153–165, Trauner Verlag, Reihe Informatik 47 (2018)
11. Schoitsch, E.: Beyond Smart Systems – Creating a Society of the Future (5.0): Resolving Disruptive Changes and Social Challenges. In: IDIMT 2019, Proceedings, pp. 387–400, Trauner Verlag, Reihe Informatik 48, (2019)

12. Deahl, D.: The Verge, "Volvo's self-driving cars are having trouble recognizing kangaroos, 3 November 2017. https://www.theverge.com/2017/7/3/15916076/volvo-self-driving-cars-trouble-recognizing-kangaroos. Accessed 24 Feb 2020
13. Koopman, P., et al.: A safety standard approach for fully autonomous vehicles. In: International Conference on Computer Safety, Reliability, and Security. Springer (2019)
14. Koopman, P., Wagner, M.: Autonomous vehicle safety: an interdisciplinary challenge. IEEE Intell. Transp. Syst. Mag. **9**(1), 90–96 (2017)
15. Whitepaper "Safety first for Automated Driving", by an industrial group with APTIV, AUDI, BAIDU, BMW, CONTINENTAL, DAIMLER, FCA, HERE, INFINEON, INTEL and VOLKSWAGEN (2019)
16. ISO DTR 4804: Road vehicles – Safety and security for automated driving systems – Design, verification and validation methods, WD, (2020, under development)
17. ISO DTR 4609: Road vehicles – Report on standardization prospective for automated vehicles (RoSPAV), (2019 under development)
18. Informatics Europe & ACM Europe: When Computers Decide – European Recommendations on Machine Learned Automated Decision Making (2018). https://www.acm.org/binaries/content/assets/public-policy/ie-euacm-adm-report-2018.pdf
19. EC: Ethics Guidelines for Trustworthy AI, HLEG AI, (2019). https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
20. Federal Ministry of Transport and Digital Infrastructure, Germany, Ethics Commission – Automated and Connected Driving (2017). https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission-automated-and-connected-driving.pdf?__blob=publicationFile
21. Von der Leyen, U.: A Union that strives for more – My agenda for Europe (2019). https://www.europarl.europa.eu/resources/library/media/20190716RES57231/20190716RES57231.pdf
22. Shan, L., et.al.: A survey on the applicability of safety, security and privacy standards in developing dependable systems. In: Proceedings of Safecomp Workshops, LNCS, vol. 11699, pp. 74–86. Springer (2019)
23. ISO/CD TR 4609: Road vehicles – Report on standardization prospective for automated vehicles (RoSPAV) (under development), by ISO TC22 AG1 (ADAG)
24. Draft Recommendation on Cyber Security of the Task Force on Cybersecurity and Over-the-air issues of UNECE WP.29 GRVA 01-17, 01-18, (2018). https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf
25. Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA 01-18, (2018). https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-18.pdf
26. Zendel, O., et al.: WildDash - Creating Hazard-Aware Bencmarks: The European Conference on Computer Vision (ECCV), pp. 402–416 (2018). http://openaccess.thecvf.com/content_ECCV_2018/html/Oliver_Zendel_WildDash_-_Creating_ECCV_2018_paper.html; https://wilddash.cc/about. Accessed March 2020
27. Granig, W., Jaksic, S., Lewitschnig, H., Mateis, C., Nickovic, D.: Weakness monitors for fail aware systems. In: Safecomp 2020, to be published in Springer LNCS