IDIMT 2016 Proceedings: http://www.idimt.org/sites/default/files/IDIMT_proceedings_2016.pdf
Trauner Verlag, Schriftenreihe Informatik 45, 2016, p. 405-423, ISBN 978-3-99033-869-8

AUTONOMOUS VEHICLES AND AUTOMATED DRIVING STATUS, PERSPECTIVES AND SOCIETAL IMPACT

Erwin Schoitsch

AIT Austrian Institute of Technology GmbH (Vienna)

(erwin.schoitsch@ait.ac.at)

Keywords

Automated driving, ADAS, road safety, connected car, cyber-security, Cyber-physical Systems, Safety, Security, Systems-of-Systems, societal impact, liability, ethical aspects, legal aspects

Abstract

Autonomous systems, automated vehicles in general and particularly the most popular concept of Automated Driving are not just a vision of a remote future – rather closed systems like metros and similar rail systems, air traffic, large logistic systems in storehouses and highly automated production lines have already autonomous systems in use. In open systems like road traffic, only first trials are under way, under severe restrictions. But all large automotive OEMs are active in this field since many years, building on the increasing number and capabilities of ADAS, Advanced Driver Assistance Systems, already in use or implementation.

Topics addressed are the European and national Roadmaps on Automated Driving or general on automated vehicles, the impact on transport in general (not only road traffic but also intermodal transport modes), and the potential benefits and threats to society and business. This includes increase of mobility to people not allowed or able to drive, the environmentally fascinating aspect of considerable reduction of the number of vehicles because of better utilization of vehicle fleets, new chances for transport optimization and reduction of resource usage, but also severe threats expected from the safety, cyber-security and privacy side of such highly automated, connected systems. Businesses will change dramatically, some becoming obsolete, but also new ones will be created. Additionally, legal, liability and even ethical aspects have to be taken into account.

1. Introduction – Autonomous Systems on the Rise

Automated driving and automated vehicles are not just a vision of a remote future – rather closed systems like metros and similar rail systems, air traffic, large logistic systems in storehouses and highly automated production lines have already autonomous systems in use. In open systems like road traffic, only first trials in public transport are under way, mainly on separated or predefined lanes, and prototypes of several manufactures in small numbers as trials.

There are several European and national Roadmaps on Automated Driving or general on automated vehicles around, including three from Austria, a short overview will be provided discussing state-of-the art, challenges for Research, Development and Innovation and, in the end, practical implementation for public use. A five-level approach from the conventional car to the fully automated autonomous (driverless) car is already defined e.g. by SAE International, formerly called "Society of Automotive Engineers" (USA). This will have huge impact on road transport in the future, but also on multi-modal transport with free interchange between modes of transport, since the driver is no longer bound to his own car he is owing but can take any transport mode, e.g. high speed trains for long distance transport, and call for an automated vehicles at his final destination for the "last mile". Besides comfort and enabling efficient road transport particular in cities even for people not being allowed or able to drive, another fascinating aspect to achieve a sustainable urban transport system is the chance to reduce considerably the number of vehicles required because they could be called on demand and after a drive do not occupy parking space for a long time because they will continue with their next order. This requires not only a considerable amount of functionality, sensors, actuators and control devices, situation awareness etc. but also integration into a new type of critical infrastructure based on communication between vehicles, and vehicles and infrastructure, and regional traffic control centers to optimize traffic as a whole and not just locally in the environ of the vehicle. A similar, but not so drastic effect is to be expected in other domains of application of highly automated or autonomous systems (industrial, rescue, health). This will make several businesses obsolete, but also create new ones which are taking up the new chances.

The author has used the example of Autonomous Vehicles for his lecture on "Emergent and Convergent Technologies" at the University of Applied Sciences FH Technikum Vienna as the topic for the scientific homework of his students, under the assumption that autonomous vehicles are operational in use with a very high coverage, raising the questions:

- Which markets will be disrupted?
- Which new markets will emerge?
- What are the major societal impacts and consequences? (benefits, risks)
- Liability, ethical and legal aspects
- What would you address for your (potential) business (niche) in this context?

which received high interest and raised some discussions and interesting answers.

Demanding challenges have to be met by research, engineering and education. Smart (embedded) systems (CPS – Cyber-physical Systems, combined building "Systems-of-Systems") are regarded as the most important component and driver for industry in this area. They are a targeted research area for European Research Programmes in Horizon 2020, particularly in the industry-driven ECSEL Joint Undertaking Initiative (ECSEL JU, 2014), and in several dedicated Programmes (PPPs – Public-Private Partnerships like the "Green Cars Initiative", euRobotics and the Electric Vehicles Initiatives). The European Commission has created the concept of the JTI (Joint Technology Initiative) ECSEL (Electronic Components and Systems for European Leadership) as a Joint Undertaking (JU), which in fact is integrating the three ETPs (European Technology Platforms) ARTEMIS-IA (ARTEMIS-IA 2016), EPoSS (EPoSS, 2009) and ENIAC (ENIAC, 2010).

In Austria, an Action Plan "Automated Driving" was initiated by bmvit (bmvit 2016), the Federal Ministry of Transport, Innovation and Technology, jointly initiated by experts from the Mobility and the ICT Division, based on the available work particularly in Austria on Roadmaps towards automated driving as mentioned before, including all major players in Austria, among them the ECSEL Austria Association. The Action Plan identified 7 "Use Cases", and in the first Call for

Automated Driving Proposals for "Testenvironments for Automated Driving" three Use Cases were selected:

- Safety by "Look-around" (vehicle-centric, sensors, actors and situation awareness, ADAS Testlab using simulation and a real environment))
- "New Flexibility": automated and connected vehicles allowing high flexibility in intermodal transport
- "Well supplied": automated and networked freight transport and logistics improving supplies and reducing critical resource requirements for a higher quality of life.

In the first Call several studies are expected how to best address these issues (probably five), in September a follow-up Call is planned for full project proposals (probably three). These three use cases meet very well what will be expressed as benefits of automated driving in this paper.

2. Evolution towards Fully Automated Vehicles – Roadmaps

The Austrian Research, Development and Innovation Roadmap for Automated Vehicles (see ECSEL Austria (2016)) took into account several existing roadmaps from different organisations with different focus and derived particularly for the Austrian situation what is relevant for R&D&I in Austria to meet the challenges of the future for Austrian industry. In the Automotive sector, Austria has no large OEM but a very strong industrial supplier base for international OEMs which is an enormous economic factor in Austria. Before the growth of the supply industry in Austria, which started a few decades ago, Austrian imports of automotive vehicles contributed very much to a negative export/import balance, but nowadays the automotive sector provides a positive contribution.
The main roadmaps taken into account were:

- EPoSS –European Roadmap on Smart Systems for Automated Driving (EPoSS (2015))
- ERTRAC – Automated Driving Roadmap (ERTRAC (2015))
- AustriaTech – C-ITS Strategy Austria (in publication), (AustriaTec (2016))
- A3PS – Austrian Eco-Mobility Technology Roadmap 2025plus (A3PS (2016))

Of course, there are some other visions and recommendations, e.g., from the AIOTI Alliance for Internet of Things Innovation, who provided several reports with recommendations for upcoming EC-programmes in the IoT sector, among those one of WG 09 on "Smart Mobility" (Oct. 2015), or from the 5G groups on "5G Automotive Vision" (ERTICO ITS Europe, 5G-PPP (2014)), arguing that 5G is a most important precondition for extensive Vehicle-to-Vehicle and Vehicle-to-Infrastructure communications in densely populated areas. Besides Automotive, the roadmap is in general on automated vehicles, e.g. it includes sections on railways, UAVs (Unmanned Areal Vehicle) and Aerospace, waterways, off-road equipment and mobility infrastructure, the last being important for effective regional traffic optimization. A few selected typical results of these documents will be explained.

The basis for most considerations are the five levels of Driving Automation for On-Road Vehicles as defined by SAE (according to SAE J3016 (2014)), (see Figure 1). Most ADAS systems are on level 2, a few may be considered having reached level 3 (automatic Jam-Control, Parking Assistant, Emergency Stops, Lane Keeping):

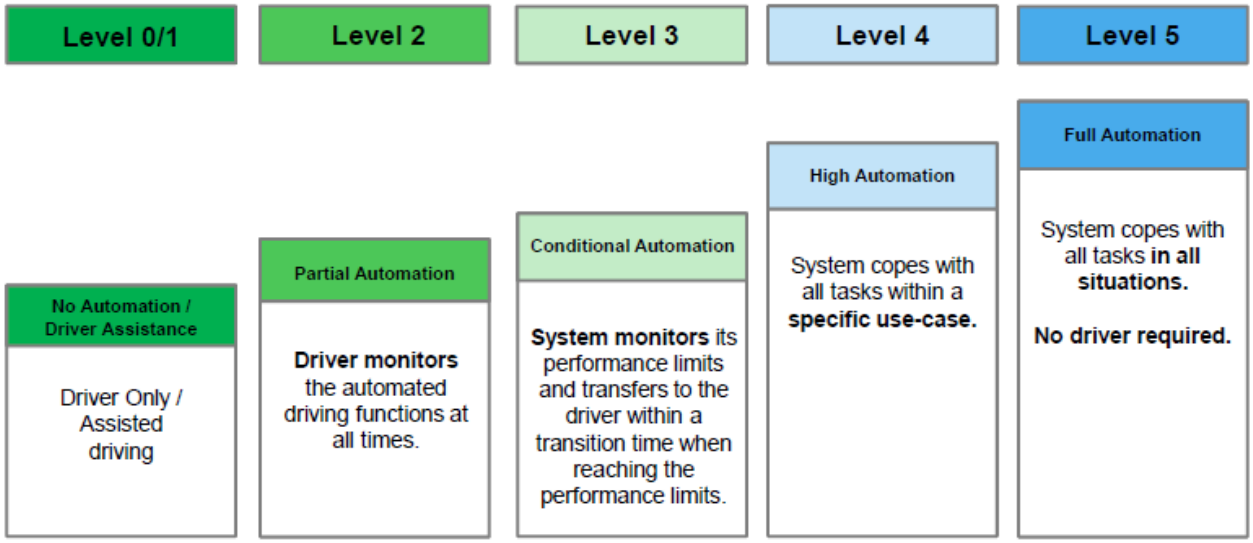


Figure 1: Levels of Automated Driving (SAE J3061) (see SAE (2014))

In more detail, the levels are described in the following table:

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	*Monitoring* of Driving Environment	Fallback Performance of *Dynamic Driving Task*	System Capability *(Driving Modes)*
***Human driver* monitors the driving environment**						
0	**No Automation**	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	**Driver Assistance**	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	**Partial Automation**	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes
***Automated driving system* ("system") monitors the driving environment**						
3	**Conditional Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the dynamic driving task with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes
4	**High Automation**	the *driving mode*-specific performance by an automated driving system of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes
5	**Full Automation**	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**

Copyright © 2014 SAE International. The summary table may be freely copied and distributed provided SAE International and J3016 are acknowledged as the source and must be reproduced AS-IS.

Table 1: Role of Human Driver and Automation in Automated Driving, Levels 0 – 5.

State-of-the-Art is at the moment Level 1 and 2, and partially Level 3 ADAS systems and combination of such systems. Claims of some car manufacturers to provide more capabilities in a serial production car are not proven to fulfill these functions under all foreseeable environments and

conditions, or are not sufficiently tested, as the recent TESLA incident demonstrates which happened in Autopilot mode and the driver not taking care of his duty to be attentive as was expected under the current law and driver's manual of Tesla. It proves that the functional safety requirement for high ASILs which are still dependent on the property of "controllability" (of the driver in a failure situation) may not be sufficient if such a "foreseeable misuse" of a driver over-relying on the a long time sufficiently working autopilot really happens (and this is "foreseeable"). The incident is still under investigation in detail, but it seems that the vision system is under certain conditions not able to identify properly a vehicle passing from the side on a crossing (see report on http://www.ntsb.gov/investigations/AccidentReports/Pages/HWY16FH018-preliminary.aspx). The only slightly damaged semi-trailer is shown in Figure 2), the Tesla went under this trailer without identifying the obstacle as such, killing the driver.

Figure 2: Shows the right side of the semitrailer at point of impact

This incident, although the first of this kind, which happened after about 100 Mio km of autopilot usage in total, which is not worse than the statistical average, drew a lot of attention on the subject and the trust in fully automated driving was at least shaken. The unfortunate vehicle after the accident is shown in Figure 3.

Some serious calculations resulted in the fact, that about 100 Mio km automated road driving is necessary to provide statistically relevant trust that the fully automated vehicle drives not less safe than a human driver! This is a severe barrier to real-world testing, and additional test by simulation and virtualization are necessary (the Austrian Automated Driving Test Environments Projects in the current Call mentioned before are aiming at that).

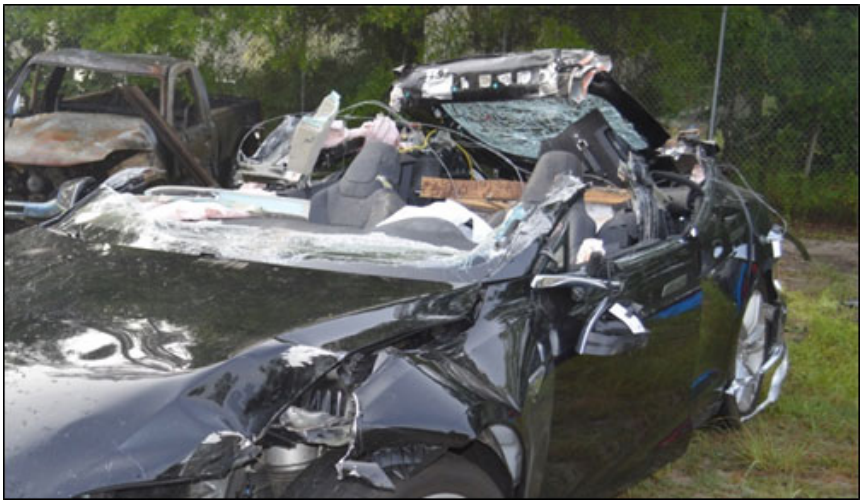


Figure 3: The unfortunate Tesla S - Passenger car damage from impact with semitrailer. (Source: Florida Highway Patrol.)

3. Stepwise Implementation and Legal Situation

The implementation therefore is planned stepwise – first automated functions will be enabled and allowed stepwise for use in low speed and well-structured environments:

1. Low speed: parking, jam control
2. Structured environment: Highway pilot (on highways only)
3. Urban traffic, the most complex one because of many non-automated systems (vulnerable road users like bicycles, people, many crossings and intersections etc.)

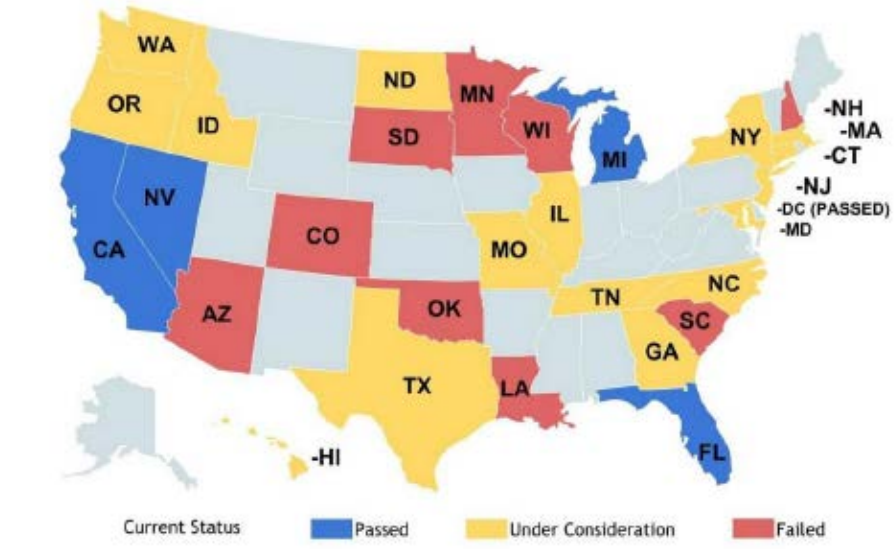
The legal situation is not appropriate for a short-term take-over of high-level automation in driving. The "Vienna Convention" from 1968 assumes and requires full control of the driver over his vehicle at all times, no automation systems interfering (not available at this time). An UN-Update (UN R 79) for steering equipment allows automated steering only at speed up to 10 km/h, aiming mainly at parking maneuvers. For autonomous cars with automated driving special conditions are set for prototypes, but always a human driver with driver's license has to be on board and be able to take over control if necessary. Even for the testing environments on public roads in Austria some adaption and legal preconditions will be set up.

The Vienna Convention is not ratified in all countries, but vehicles have to be built according to these rules for export purposes and de facto it is accepted in most national laws (see Figure 4). For partial automation, when the driver monitors continuously and can take over control anytime, no conflict with the Vienna Convention is encountered. For higher automation, an adaptation or interpretation is necessary for legal reasons.

In US, there is the situation quite different in different states: In some states, highly automated cars are allowed, but under certain restrictions (see Figure 5):

- Presence of driver able to take over
- Easy to switch between driving modes
- Data logging (to be able to reconstruct incidents and clarify rather complex liability issues)
- Different license plates to signal to other road users that automated mode may be used
- Additional/different insurance conditions

Figure 4: Status of ratification/signed of the Vienna Convention (Austria ratified 1981), Source Wikipedia 2015



[Source: Wikipedia, October 2015]

Figure 5: Current status in US: Automated Driving passed, under consideration and failed (2015)

A nice example of different license plates is shown in Figure 6 (source: Wikipedia 2015)

Figure 6: License plates in Nevada: left regular, right „Autonomous Vehicle“

4. Highly Automated and Autonomous Systems – the Cybersecurity Threat

4.1. Highly automated systems – Cyber-security Vulnerability and Privacy Violation

We have to tackle particular aspects of the three levels of software-intensive networked, highly integrated embedded systems which build the autonomous systems. These levels are known as

- Embedded systems (software-intensive systems, integrated in a hidden or visible manner in everyday devices, mobile or fixed, inside or outside us)
- Cyberphysical systems (combined complex embedded systems with sensors, actuators, integrating physics, mechatronics, intelligence, decision-making and perception)
- Systems – of – systems (aggregation of systems, composed of interconnected autonomous systems originally independently developed to fulfil dedicated tasks.

The design, operation, and protection, but also risk assessment, validation, verification and certification, maintenance and modification throughout the life cycle of these systems have to take into account the interplay between humans, environment and systems. Systems must be robust to cope with these problems in an adaptive manner ("resilient systems") (Schoitsch, (2013), (2015)).

Massively deployed autonomous or highly automated systems applications of high potential for safety, security and privacy risks are arising in context of

- The grid control approaching private homes: smart grids for efficient power distribution, but our civilisation is very sensitive on loss of power because of almost all services and protective measures depend on appropriate power availability – on the other hand a lot of data on individual behaviour, habits, information on presence and absence etc. become available, endangering privacy, in:
    - Building automation and control (heat, cooling, elevators, fire alarm and fire fighting, doors/entrance and rescue), at least with remote maintenance access,
    - AAL (Ambient Assisted Living) and health-care (from remote monitoring to automatic or triggered intervention),
- Highly automated process industry plants, power plants and manufacturing plants, even with remote "control via internet", and particularly autonomous but interconnected systems, e.g. robots, cooperating with each other and humans,
- Large machinery and construction vehicles operating (semi-) autonomous, service robots in human populated environment and robotic farms, off-road vehicles and equipment,
- Transport, particularly road vehicles utilizing car2car and car2infrastructure communication for (semi-) autonomous driving, platooning and road safety in general; security and particularly privacy are endangered.

For the purpose of this paper, particularly the last two bullet points are of interest: The highly automated car (not only the connected one in Car2Car and Car2Infrastructure, but already single cars with some IP-based connections for human communication and entertainment) has shown sever vulnerabilities because of incomplete separation of driving/car automation & control systems and entertainment, communication and maintenance systems.

4.2. Integration into a critical infrastructure – Safety and Privacy Violation

V2V and V2I (often generalized by V2X or C2X) are expected to make future road traffic much more efficient and safe, and many (research) projects, prototypes and evolving communication standards are engaged in this direction, with the final goal of truly autonomous driving; the first

step would be platooning of "car trains" on high ways ("Highway Pilot"), i.e. a bunch of vehicles following a lead vehicle autonomously, controlled by information via V2V communication, and supported by a number of sensors controlling near distance behavior and safety.

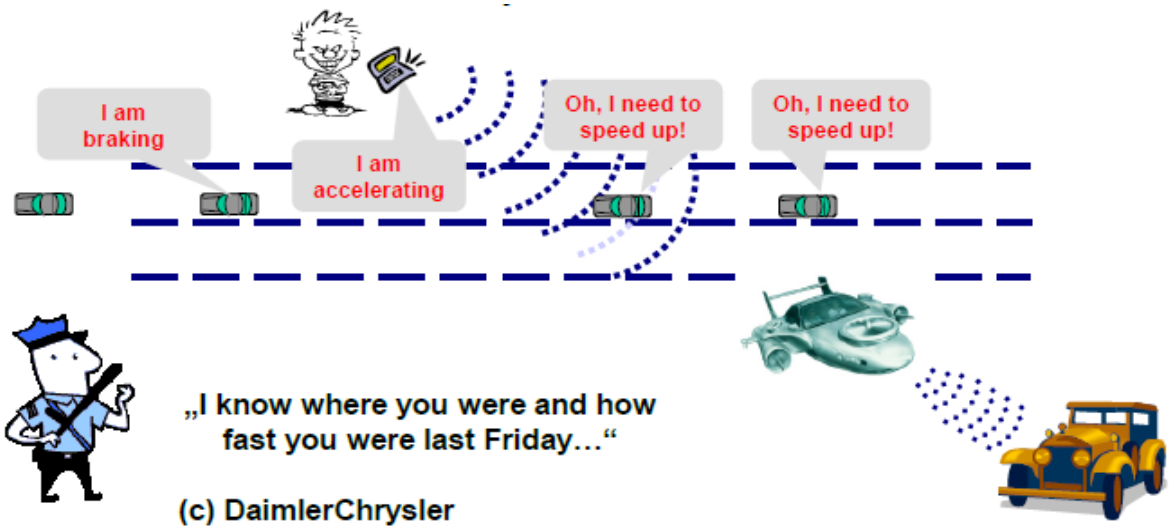


Figure 7: Platooning road traffic: safety, security and privacy issues

This concept implies a number of safety, security and privacy issue (see Figure 3) – and the liability issue is far from being resolved legally (who is responsible in case of an accident? The first driver? How strong is the individual driver in control of his vehicle, how can alertness be guaranteed?). An additional problem is the long-term guarantee of security, keys can be broken, electronics can wear out partially, there must be alternatives in case a car is used ten years or longer, with the same devices inside or not, etc.).

4.3. Safety and security risks through Maintenance

Imagine that manufacturers of cars see advantages in doing of remote maintenance (update) of in-car software (updates, error corrections) in the field via wireless communications to avoid expensive call-back. It works (sometimes) with space vehicles and satellites – why not for cars? (see Figure 7) (Schoitsch (2015)).

Here again, the hazards and risks need very thorough analysis – it has to be guaranteed that only in a safe situation and in a secure manner downloads of proven updates for the actual configuration of software in the individual car are possible, taking into account many complex scenarios – just to download when the car is not moving is for sure not sufficient, since many scenarios can be imagined where cars stop, but have to restart immediately if required by the traffic situation (Schmittner, 2015).

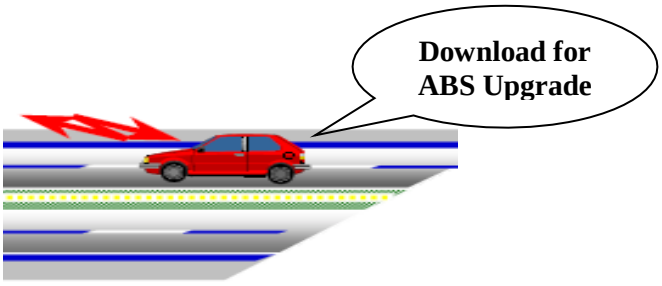


Figure 8: Software download in the field?

At the moment, this is only possible in a standardized way via diagnostic interfaces in a qualified maintenance station. But several automotive OEMs already supply critical updates via over the air update systems. As an example, the security vulnerability in the BMW ConnectedDrive was resolved by sending a security patch via the BMW ConnectedDrive system (BMW, 2015).

5. The Highly Automated and Connected Car: A Hacker Paradise?

The most fascinating aspect of connected cars and highly autonomous driving is the chance to achieve a sustainable urban transport system by reducing considerably the number of vehicles required because they could be called on demand and after a drive do not occupy parking space for a long time because they will continue with their next order. This requires not only a considerable amount of functionality, sensors, actuators and control devices, situation awareness etc. but also integration into a new type of critical infrastructure based on communication between vehicles and vehicles and infrastructure, and regional traffic control centers to optimize traffic as a whole and not just locally in the environ of the vehicle.

5.1. Modern Cars: Increased attack surface of an "open system"

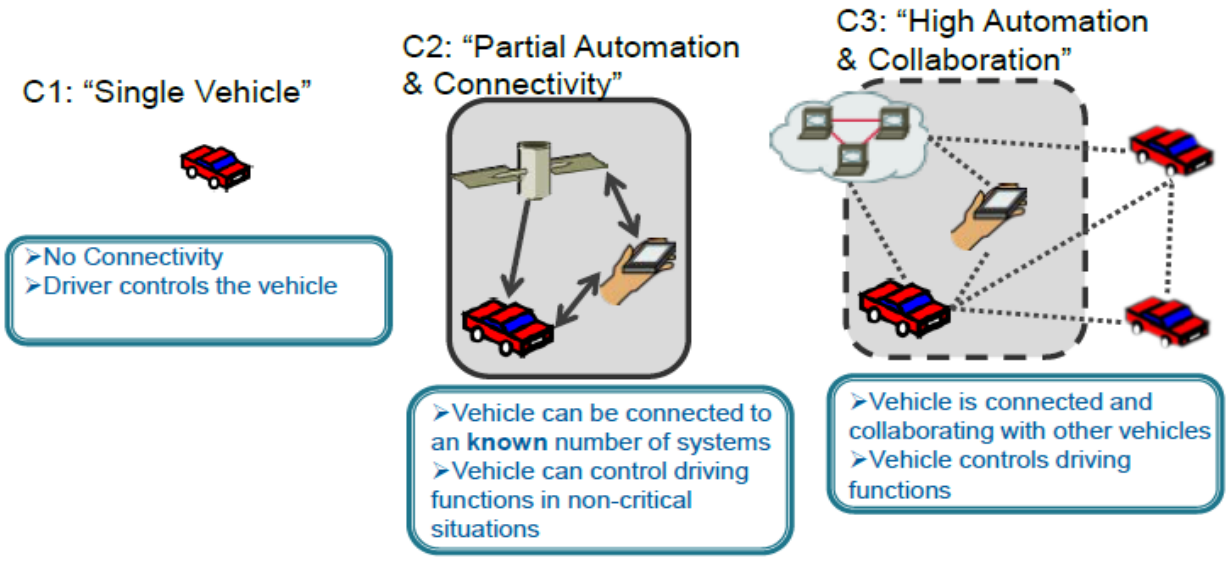


Figure 9: „Open System" car – single vehicle and connected vehicles - increased attack surface, privacy

Any modern car, even if not "connected" or "highly automated", has many access points for control from outside with safety and security impact (Figure 9). We have to consider three different levels of automation with increasing order of complexity and risk of cyber-attacks.

In TU-Automotive (2016), an example map of electronic systems in a modern car is shown – all of them connect in various ways and potential targets of attacks, often via curious paths and accidental knowledge (see Figure 10).

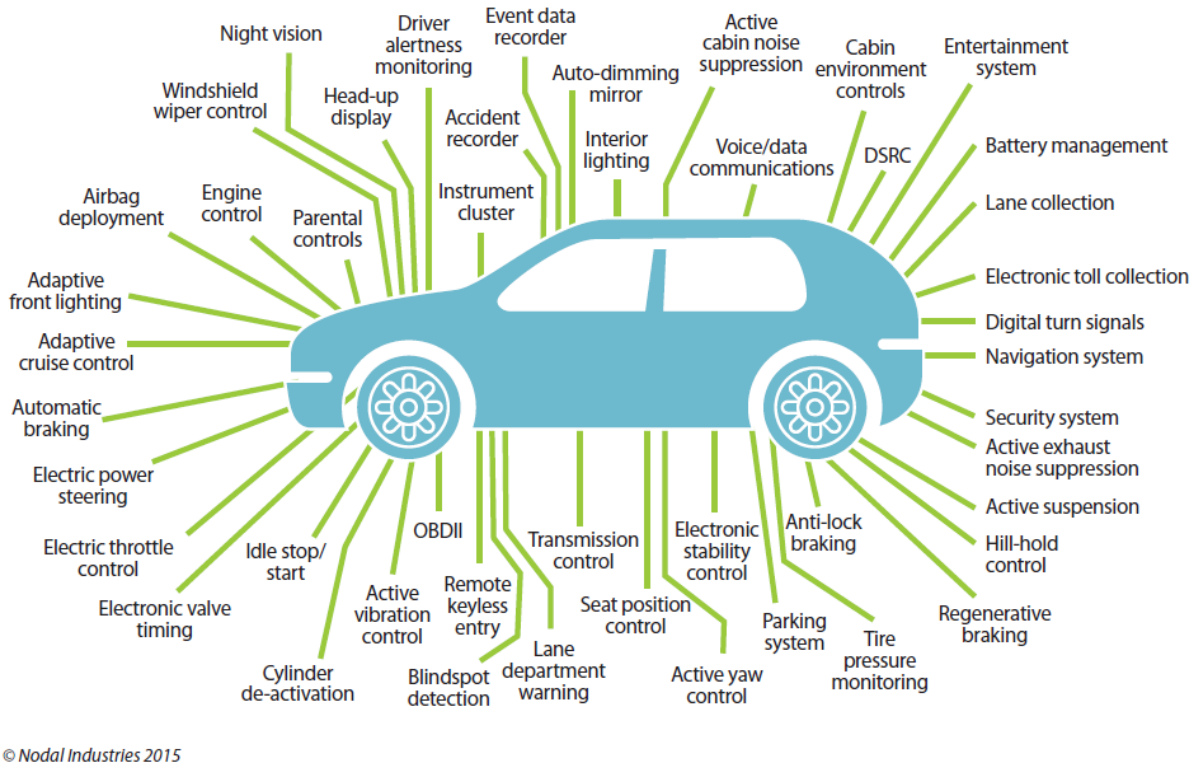


Figure 10: Example map for E/E/PE functional units in a modern car – connected and potential attack targets

A model to understand hackers' motivation and draw a conceptual diagram of threats is provided by Schneider (1999), which should help to systematically describe the problem (Figure 11).

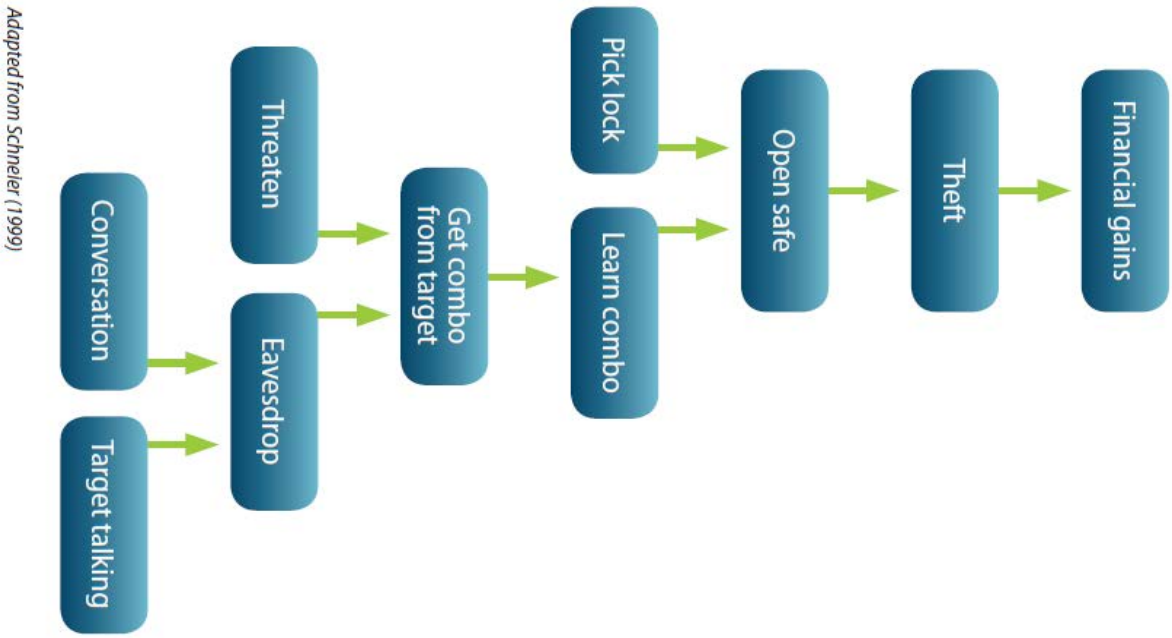


Figure 11: Attack tree documenting a safe-cracking as an example

The report analyses the hackers motivations (different hacker types: Tuners (of engines etc. by electronic means), academic security researchers (mainly positive to detect vulnerabilities or develop countermeasures), white hat hackers (often employed to identify weaknesses), black hat

hackers (use similar tools as white hat hackers, but with criminal intent), grey hat hackers (ethically questionable), vehicle theft (stolen by order), financial theft and damage (and blackmail), remote surveillance of people and spying) and attack targets. These are units, buses and communication means and are analyzed in some detail: Bus bridges, infotainement, OBD-II (diagnosis and maintenance), Bluetooth, Wi-Fi, CAN Bus, dedicated smart phone interfaces, TPMS (Pressure Monitoring System), Immobilizer (see Schoitsch (2013), several possible attack targets), telematics manufacturer and after-market telematics (adds additional risk afterwards by using legally interfaces), passive keyless entry and start systems, e-Call, various ADAS system features, DSRC (Digital Short Range Communication) and Sensor Networks. If we look at this list and the detailed discussion what already has happened in the past we have a rich menu for Hackers – an ideal Hacker Paradise!

5.2. Some popular examples of "Hacks"

5.2.1. The Jeep Cherokee Case

In "Wired", 2015, Andy Greenburg reported his experience on sitting in a hacked car (although he knew that it will be hacked, so there was no real surprise – only the surprise how far this is possible to manipulate his Jeep Cherokee via remote hacking) in an article „Hackers remotely kill Jeep on the highway – with me in it". Imagine, if that happens unexpectedly! Panic is the least result!

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

It was done stepwise: The hackers, Charlie Miller and Chris Valasek, started with uncritical effects, then increased the pressure on the driver via remote control:

- Stepwise take over: driver could not interfere by manual control of vents, radio ultra loud, wind shield wipers
- Photo of hackers appeared on car display
- Interstate 64 ramp: speed control, braking lost
- Commandeered steering wheel
- Then stopped action when Alan cried for help.

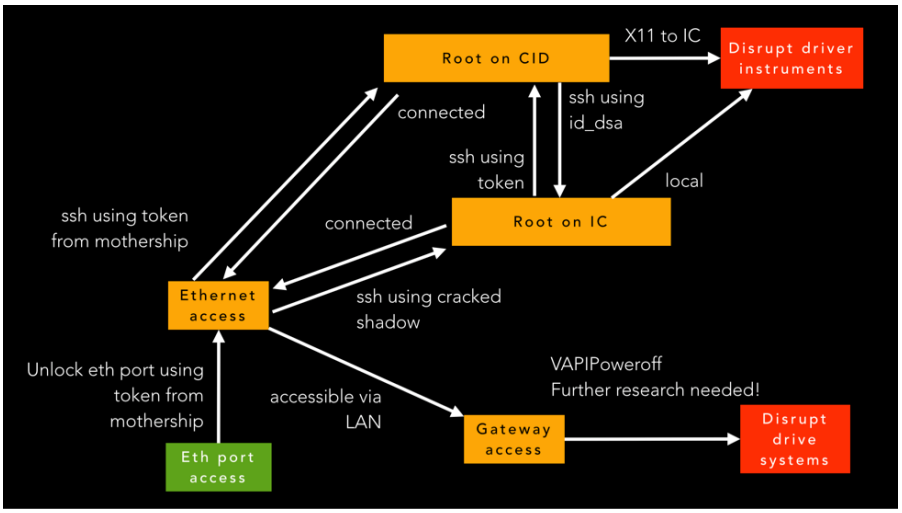
Figure 12: The hackers in action – and the end of the story (fortunately done in a controlled manner)

5.2.2. A few other examples:

- **Corvette: Control brakes via insurance OBD dongle**

http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget

- **Tesla: Remote manipulation of instruments or drive systems**



https://blog.lookout.com/blog/2015/08/07/hacking-a-tesla/

- **VW: Disable Airbags via manipulated USB flash drive**

http://www.theregister.co.uk/2015/10/23/hackers_pop_mechanics_laptops_to_silently_disable_car_airbags/

- **Nissan Leaf Electric Car Hack Vulnerability disclosed**

http://www.bbc.com/news/technology-35642749
http://www.troyhunt.com/2016/02/controlling-vehicle-features-of-nissan.html

  - Vulnerability communicated to Nissan on 23. Jan by Troy Hunt
  - Remote Access to charging, climate control, driving history
  - Vulnerable Service deactivated on 25 Feb

6. Existing and Upcoming (Automotive and Industrial) Security Standards

Security standards like ISO 15408 (Common Criteria - CC) defines EALs (Evaluation Assurance Level EAL 1 - 7, quite different from the ISO/IEC 61508 group probabilistic risk levels (SIL 1-4), which are not applicable to security). This standard helps evaluate, validate, and certify the security assurance of a technology product against a number of factors, such as the security functional requirements specified in the standard. Hardware and software can be evaluated against CC requirements in accredited testing laboratories to certify the exact EAL (Evaluation Assurance Level), i.e. its product oriented. Requirements for evaluation become stricter from EAL1 - Functionally tested, EAL2 - Structurally tested, EAL3 - Methodically tested and checked, EAL4 - Methodically designed, tested and reviewed, EAL5 - Semi-formally designed and tested, EAL6 - Semi-formally verified, designed and tested, to EAL7 - Formally verified, designed and tested.

ISO 27002 (formerly ISO/IEC 177799) establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It contains best practices of control objectives and controls in information security management and looks at security from a systems perspective, not only IT devices.

IEC SC65C Standards: Industrial networks (covering industrial communications security)

This subcommittee handles an enormous number of standards and subparts of standards on (industrial) buses (field bus standards, real-time Ethernet, etc.). Very important for the safety and security aspect is the series IEC 61784 (Industrial communication networks – Profiles), particularly (1) Profiles for real-time networks (IEC 61784-2), (2) functional safety fieldbuses (IEC 61784-3-xx) and (3) IEC 61784-4 - Profiles for secure communications in industrial networks

IEC TC 65 WG 10 – IEC 62443 and ISA 99 standards: a major activity is centred around the series of IEC 62443 - Industrial communication networks - Network and system security, consisting of

several parts, including e.g. System security requirements and security assurance level, Patch management, and Certification of IACS supplier security policies and practices, focused on system level security (not fieldbuses). This work is now done in close co-operation with ISA (Instrument Society of America, ISA 99 committee). IEC 62443 defines 4 SLs (Security Levels) which are of qualitative nature based on the level of efforts and skills required to successfully attack a system:

- SL1: casual or coincidental violation
- SL 2: simple means: low resources, generic skills and low motivation
- SL 3: sophisticated means: moderate resources, IACS-specific skills and moderate motivation
- SL 4: sophisticated means: extended resources, IACS-specific skills and high motivation

Functional Safety Standards for several domains based on the generic basic safety standard ISO/IEC 61508 have evolved since 2000 after IEC 61508 Ed. 1 was completed. The automotive functional safety standard ISO 26262 Ed. 1.0 was published 2011 (parts 1-9) and 2012 (part 10).

The functional safety standards of the first generation did not tackle the challenges of highly connected "systems-of-systems". Security in an open vehicle system will now become a new factor to be considered in system engineering and safety analysis.

IEC 61508 Ed. 2.0, finished 2010, took as first functional safety standard into account that security may impact safety of a system. Therefore it requires consideration of security threats ("*malevolent and unauthorized actions")* in risk and hazard analysis, with accompanying measures to be undertaken throughout all lifecycle phases. A security threat and vulnerability analysis should be conducted if a security threat is identified as a potential cause for a hazard in order to specify security requirements (IEC 61508, Part 1, 7.5.2.2). Security has then to be reflected in the safety manual as well (Part 3, Annex D 2.4). In notes are definitely addressed IEC 62443 and ISO/IEC TR 19791 (Part 1, 1.2, k) for guidance on details.

In the preparation phase of IEC 61508-3 Ed. 3.0 (Software part) it was decided to look at the ongoing activities in IEC with respect to "security-aware safety" and to provide more mandatory and informative guidance on a coordinated approach to security in context of functional safety.

In IEC TC65 (Industrial-process measurement, control and automation) considerable concerns arose with respect to the safety impact of security issues in industrial automation systems. An Ad-hoc Group (AHG1- "Framework towards coordination of safety and security") was founded to look into the issue and provide recommendations how to handle the co-ordination of security issues in functional safety standards. It has finished its work with a report and recommendations, and started as IEC TC65 WG 20, "Bridging the requirements for safety and security", writing a TS (Technical Specification) on this topic.

David Strickland, Chief Administrator for the National Highway Traffic Safety Administration (NHTSA), stated: *"…electronics systems are critical to the functioning of modern cars, and are becoming increasingly interconnected, leading to different safety and cyber security risks. (…) With electronic systems assuming safety critical roles in nearly all vehicle controls, we are facing the need to develop general requirements for electronic control systems to ensure their reliability and security".*

The Austria proposal for ISO 26262 to include the interface between safety and security in the functional safety standard for road vehicles was taken up and led to contributions of a task group to ISO 26262 Part 2 (Management of functional safety) and Part 4 (Product development at system level) , now included in the DIS (Draft International Standard).

Additionally, ISO TC 22 SC 32 started TWO new work items on the same topic, one from the German DVA and DIN on "Road vehicles – Automotive Security Engineering" and SAE on "Road

vehicles – Vehicle Cybersecurity Engineering", based on the existing SAE Guideline J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems). Both were accepted, but only one standard is envisaged, and the most important question is which approach to follow. Whereas the German proposal tends towards an independent Cybersecurity Standard, not considering the safety impact, the SAE proposal takes up both: a safety-related part where both sides (safety and security) are taken into account following ISO 26262 life cycles, and a security related part, where issues like privacy and confidentiality without safety impact are handled. In the procedural vote, the Austrian group from AIT proposed the following, tending to the SAE approach:

"Austria approves the resolutions C893(explanation: merge both NWIP) and C894 (explanation: NWIP should fall under PSDO – Partner Standard Development Organization Agreement – between ISO and SAE, to get highest acceptance in the world) but would like to remark that the combined approach should follow mainly the direction proposed in NWIP3586. It is of utmost importance to consider safety in the cybersecurity process and to follow an engineering approach suitable for the automotive domain. While cybersecurity may require some extensions, especially in the maintenance and operations phase it should, in our opinion, in general follow the ISO26262 lifecycle. Safety and Security is required for issues like advanced driver assistance systems with communication features. While additional issues are also relevant for security the primary goal are safe vehicles. The approach proposed in SAE J3061, to describe a combined process for safety and security critical systems and only use a stand-alone cybersecurity process for systems without safety relevance should be adapted for the new standard.

Austria disapproves resolution C895 (explanation: German lead, kick-off in Munich) and would prefer a Kick-Off Meeting organized by the US. US led the effort on the J3061 which has been well received and should therefore also lead the Cybersecurity NWIP."

Hopefully, the new standards, ISO 26262: 2018 for functional safety and the Vehicle (Automotive) Cybersecurity Engineering Standard will facilitate safe as well as secure automotive systems!

7. Business, Legal and Societal Impact

In this chapter, a short overview is given on some business, legal and societal issues that will be impacted by autonomous vehicles if they are massively deployed and used.

7.1. Disrupted Markets and New Business

Several markets will be disrupted – services connected with driving a car will be reduced if automated vehicles fulfil their missions without any staff – only when loading and unloading people will still be necessary, but only the sender and receiver of freight need to be there. Taxi drivers will oppose such changes (as they do now with respect to Uber, or in the past the coachmen against railways). Public transport will change as well – bus lines in areas which are not densely populated will be replaced by "automated cars on demand", the structure of public transport networks will change. The role of traffic police will change as well – maybe they will have to become support staff for the automated vehicles in case of defects etc.

OEMs have already started to think about their changing role: the result of a large number of autonomous vehicles used on demand should reduce considerably the number of vehicles, but on the other hand require particular fleet management and "short-term leasing", so they could become car sharing and fleet management organizations. Service of the now more critical infrastructure will be another challenge with a positive business effect.

The service sector could change as well: Instead of people going to a shop, or to a doctor, or to a therapy, these people could come to you or even do services in the car (if equipped properly). One particular possibility could be the "emergency response" – autonomous vehicles could in case of an emergency switch to an emergency mode and transport a person as fast as possible to the nearest available hospital. A lot of nice ideas have been brought up in the discussions and the homework in my lecture at the University of Applied Sciences FH Technikum, Vienna, on "Emerging and Converging Technologies". New business models will emerge, and new products needed for these markets (besides the development, production and integration of technologies for autonomous driving!). Things we would not even imagine today could become quite normal in the future!

7.2. Liability, Ethical and Legal Aspects

One of the questions raised was on the potential impact on liability and insurance. Today, the driver has to learn and train to get a drivers' license (but since although almost everyone gets it, so the qualification is not as high as for pilots, as an example). If the autonomous car can be used by everyone, who has to get the drivers' license? Since the driver in the extreme case does no longer exist, the liability lies with the OEM (manufacturer), i.e. "the car has to do the examination to get a driver's license". Liability will be mainly with the manufacturer – VOLVO Trucks was one of the first OEMs declaring that the company will take responsibility and liability in this case.

The most critical phase will be the transition phase between conventional driving and autonomous driving which will happen continuously but need some time. There are studies in the US saying that a "conventional" driver will need particular awareness training instead of the general driving training to be able to operate the highly, but not fully automated car, because (as demonstrated by the Tesla S2 accident) alertness (and therefore controllability) is considerably reduced.

For insurance companies, the scenario will change considerably. Since today, 90% of accidents are claimed to be caused by humans, ADAS will reduce considerably number of accidents (hopefully). The consequence should be that the cost of insurance should be reduced for the driver because of reduced risk. For fully automated vehicles, the user will no longer be responsible and liable (as today in public transport means), the liability and as consequence the insurance cost will be with the OEM (manufacturer). In the long term, the insurance business in the automotive sector will be considerably reduced. The German KPMG believes that the turnover in this business will be reduced by 45% within a decade.

The legal aspects with transport safety and rules like the "Vienna Convention" have been discussed as well before.

At the moment, most effort and thoughts are on technological and liability issues – but there could be ethical issues as well, when the computers take decisions. If we construct a scenario, that the automated vehicle identifies a situation, where either the vehicle with the driver or a person on the street (or several persons, old or young) are endangered in any case – which risk to take? Is the "programmer" responsible if somebody is killed because of the decision (e.g., rather hit the older person than the younger one, or endanger the driver and the car? Can a computer be "selfish"? That's only a sketch, but it should just draw attention to this issue.

7.3. Societal Impact (Benefits and Risks)

These topics have partially already been covered in previous chapters. This includes benefits like reduction of overall resource usage, social inclusion of people like elderly ones, people with special needs and the like into the world of high mobility, transport optimization, less parking space needed in cities, better utilization of road capacity, positive environmental impact e.g. by lower emissions because of moderate automate driving behaviour. "Demographic change" is another important issue

– hopefully, the new technologies allow us to be kept longer in the loop as independent living persons! Safety and comfort are declared goals of the autonomous systems development – but this can become a threat as well!

Risks are changes in business and labour markets which are not compensated by alternative businesses and jobs, and the risk of additional safety, security and privacy violations. It is difficult today to understand and foresee how "disruptive" autonomous driving (and autonomous systems in general) will be for our society – we are now starting to hand over tasks, responsibilities and decisions to machines without being in the loop any longer!

8. Conclusions

Automated (autonomous) driving is a most significant change for society, economy, the automotive and public transport industry in its history. National programmes, particularly in Germany and Austria, but also in other European countries, and the EC in its H2020 Research Programmes (including several PPPs and the ECSEL JU) and the US National Science Foundation have both identified autonomous vehicles and systems as key research areas. Developments towards autonomous systems and vehicles are becoming increasingly important, in the first steps mostly called "highly automated". Advances are expected with respect to intervention (collision avoidance), and co-ordination (traffic management and control in air, sea and ground), with huge impact on environment and reduction of resource usage and consumption, for a better sustainable economy (ECSEL MASRIA 2014 and 2015, ARTEMIS-IA SRA 2016). Nevertheless, we have to take care that potential threats to safety, security and privacy are avoided and ethical as well as liability and legal issues resolved in time.

Just now, effort is undertaken to consider security in context of safety-critical systems and functional safety standards, particularly in IEC 61508, Ed. 3.0, in ISO 26262 (automotive) - 2018, and on a general basis in the IEC TC 65 WG 20 "Bridging the requirements for safety and security" as well as for ISO TC22 SC 32 for "Road vehicles – Vehicle (Automotive) Cybersecurity Engineering", hopefully aligned and contributing to safe and secure automated driving systems for the benefit of society and environment.

Acknowledgement

Part of the work has received funding from the EU ARTEMIS/ECSEL Joint Undertaking under grant agreement n° 692474 (AMASS), and from both, the EC ECSEL JU and the partners' national programmes/funding authorities (in Austria FFG (Austrian Research Promotion Agency) on behalf of BMVIT, The Federal Ministry of Transport, Innovation and Technology) and (grant agreements n° 332987 (ARROWHEAD) and n° 621429 (EMC²)).

9. References

5G-PPP (2014), White Paper on Automotive Vertical Sectors, available at: https://5g-ppp.eu/wp-ontent/uploads/2014/02/5G-PPPWhite-Paper-on-Automotive-Vertical-Sectors.pdf.

A3PS (2016), „Austrian Eco-Mobility Roadmap 2025plus", A3PS, Vienna, 2016, available at: www.roadmap.a3ps.at. And http://www.a3ps.at/site/sites/default/files/images/downloadfiles/a3ps_roadmap_eco_mobility_2025plus.pdf

ARTEMIS-IA (2016), ARTEMIS Strategic Research Agenda (SRA) 2016, ARTEMIS Industrial Association (Advanced Research and Technology for Embedded Intelligence and Systems), www.artemis-ia.eu

AustriaTech (2016), C-ITS Strategy Austria, in publication (2016)

bmvit (2016), Austrian Action Plan Automated Driving – Automated, Connected and Mobile, Austrian Federal Ministry for Transport, Innovation and Technology, available in German, http://www.bmvit.gv.at/service/publikationen/innovation/mobilitaet/automatisiert.html

BMW (2015), BMW Group Connected Drive increases data security. Rapid response to reports from ADAC, Germany, https://www.press.bmwgroup.com/global/download.html?textId=245368&textAttachmentId=293791, 30.1.2015

ECSEL (2015) MASRIA 2015 (Multi Annual Strategic Research and Innovation Agenda) (e.g. http://www.smart-systems-integration.org/public/news-events/news/ecsel-masria-2015-now-available-for-download)

ECSEL Austria (2016), Austrian Research, Development & Innovation Roadmap for Automated Vehicles, supported by bmvit, ITS Austria, A3PS, AustriaTech, ASFiNAG, ÖBB, FFG, Austrian Industry and Austrian research & academia, http://www.ecsel-austria.net/newsfull/items/automated-driving-roadmap.html

ECSEL JU (2014), Electronic Components and Systems for European Leadership, www.ecsel-ju.eu

EN 50129 (2003), Railway applications - Communication, signalling and processing systems - Safety-related electronic systems for signalling, 2003.

ENIAC (2010) European Nano-electronics Initiative Advisory Council, Multi-Annual Strategic Plan, www.eniac.eu

EPoSS (2009) European Platform on Smart Systems Integration, Strategic Research Agenda, http://www.smart-systems-integration.org

EPoSS (2015), "Roadmap on smart systems for automated driving", 2015, European Technology Platform on Smart Systems Integration (EPoSS).

ERTRAC (2015), "ERTRAC Roadmap Automated Driving," ERTRAC, July 2015. [Online]. Available: http://www.ertrac.org/uploads/documentsearch/id38/ERTRAC_Automated-Driving-2015.pdf.

IEC 61508 (2010), Ed. 2.0, Part 1 – 7, "Functional Safety of E/E/PE safety-related Systems", 2010.

IEC 61784 (2005), First edition. 2003-05: Digital data communications for measurement and control (many parts).

IEC 62443 (2015): Network and system security for industrial automation and control

ISO/IEC (2009) 15408-1, Information technology -- Security techniques -- Evaluation criteria for IT security (3 Parts)

ISO 26262 (2011/2012), Part 1- 10, Road vehicles – functional safety

ISO/IEC 27002 (2005) Information technology -- Security techniques -- Code of practice for information security management

Laprie, J.-C. (2005), "Resilience for the Scalability of Dependability", 4th International IEEE Symposium on Network Computing and Applications, IEEE CPS 2005, Cambridge, MA, p. 5-6, ISBN 0-7695-2326-9

Parasuraman, R. (2000), Sheridan, T. B., and Wickens, C. D., A model for types and levels of human interaction with automation. IEEE Transaction on Systems, Man, and Cybernetics, A 30(3), 286-29, 2000.

SAE (2014), Standard J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems.

Schmittner, C. (2015), Ma, Z., Schoitsch, E., and Gruber, T., "A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive Cyber-physical Systems". In: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security (pp. 69-80), ACM (April 2015)

Schmittner, C. (2016), Ma, Z., Reyes, C., Dillinger, O., Puschner, P., Using SAE J3061 for Automotive Security Requirement Engineering, in: Workshop Proceedings of the 35th International Conference on Computer Safety, Reliability and Security, SAFECOMP 2016, Springer LNCS 9923, Int. Publ. AG Switzerland, 2016, ISBN 978-3-319-45479-5.

Schoitsch, E. (2013), Safety vs. Security – Related Trade-Offs and Emergent Behaviors in Cyber-Physical Systems, IDIMT 2013, Proceedings Trauner Verlag 2013, p. 181-196, ISBN 978-3-99033-083-8

Schoitsch, E. (2015), Connected Autonomous Vehicles and Systems – Can Combining Safety & Security Standards Help to Avoid Economic Loss, Security Breaches and Catastrophes? , IDIMT 2015, Proceedings Trauner Verlag 2015, p. 477-486, ISBN 978-3-99033-395-2

TU-Automotive (2016) Hacks and Threats Report 2016, TU-Automotive Cyber Security Europe, 2016, availability: www.tu-auto.com/cyber-security-europe