SAFETY AND SECURITY THROUGH THE DESIGN OF AUTONOMOUS INTELLIGENT VEHICLE SYSTEMS AND INTELLIGENT INFRASTRUCTURE IN THE SMART CITY

Dániel Tokody[1,]*, Attila Albini[1], László Ady[2], Zoltán Rajnai[1] and Ferenc Pongrácz[3]

[1]Óbuda University, Doctoral School of Safety and Security Sciences
Budapest, Hungary

[2]Óbuda University, Kandó Kálmán Faculty of Electrical Engineering, NextTechnologies Ltd.
Budapest, Hungary

[3]IBM Hungary Ltd.
Budapest, Hungary

DOI: 10.7906/indecs.16.3.11
Regular article

Received: 21st March 2018.
Accepted: 31st August 2018.

ABSTRACT

Our article is discussing the methodical basics of planning smart mobility. Smart mobility is one the main elements of a smart system. According to the methodology presented in our article, transportation in a smart city can be developed in a safe form, focusing on two main elements: safety and security planning of smart mobility. Intelligent (transportation) infrastructures and autonomous intelligent vehicles will be integrated in a common system in order to achieve the digital transformation of the transportation system. The aim of this research is to examine questions raised in relation to the control and communication of autonomous vehicles and vehicle systems. The development of autonomous intelligent vehicles and vehicle systems is based on the further development of the cooperating intelligent transportation systems to achieve smart mobility. The research aims to find such methods and procedures which help the safety planning of increasingly complex cyber-physical systems and system elements used in autonomous intelligent vehicles and transport systems, in view of aspects of safety and operational risks.

KEY WORDS

digitalisation of transportation, autonomous intelligent vehicle, smart city, intelligent infrastructures

CLASSIFICATION

APA: 4090, 4100
JEL: R41

*Corresponding author, η: daniel_tokody@ieee.org; –;
Doctoral School of Safety and Security Sciences of Obuda University, H – 1428 Budapest, Pf.:31, Hungary

INTRODUCTION

The aim of the present research is to examine the questions raised in connection with the control and communication of autonomous vehicles and vehicle systems, the building process of autonomous intelligent vehicles and vehicle systems, the further development of cooperative intelligent transport systems and the implementation of smart mobility. Its goal is to elaborate the methods and procedures to support the safety planning of cyber-physical systems and system elements with an increasing level of complexity in the autonomous intelligent vehicles and vehicle systems, by considering such factors as operational safety, the risks of keeping in operation and cyber security. In the processing of large amount of data generated throughout the operation of intelligent infrastructures and autonomous intelligent vehicles, a key role will be given to the information created by transforming the data collected by various sensor networks. Serious predictions and important conclusions about the communication-based and networking cooperative structure of the past can be made based on such information, including with real-time or future operation of the transport system. Therefore, processing big data (data mining, data science) will provide such information which can be used to ensure safety, operation of the transport system and achieve any business objectives related to transportation.

SYSTEM ENGINEERING FOR SMART MOBILITY

Smart mobility innovation programmes can be characterized by the use of key enabling technologies, which leads to the digitalization of transportation. In order to achieve smart mobility, a holistic approach is needed in system planning, which presupposes the synergy of the interdependent systems related to the transport system (energy sector, urban subsystems, etc.) These Key Enabling Technologies are connected by the information and communication technologies, which have an important role in the digitalisation of transportation. The digital transformation of transportation can be achieved through four basic processes: automation, digital data, digital user interface and the systems interconnectivity.

Some Key Enabling Technologies of smart mobility:

- Automation – sensor and controller network, automotive sensor fusion system [1], adaptive speed control [2], on-board vehicle self-diagnostic sensor [3], Inertial Navigation Systems [4].
- Digital data – cloud technology and Big Data [5], data fusion system [1], information distribution – driver information system [3], automotive vehicle data management [6].
- Digital user interface (driver, operator, vehicles) – driver-vehicles interaction [7], task optimization [8], maintenance [9].
- Interconnectivity – vehicle fleet management systems [10], peer to peer networking [11], knowledge accumulation [12] and Artificial Intelligence [13, 14], self-configurable vehicle clusters [15].

Based on these Key Enabling Technologies, autonomous vehicles can be considered as one of the main elements of smart mobility (see Fig. 1). The level of vehicle automation has been defined by the Society of Automotive Engineers in the document entitled “Levels of motor vehicle automation adapted from SAE Standard J3016”. LoA5 (Level 5 of Automation, the full automation of autonomous vehicles) expects the development of a transport infrastructure which is completely different from traditional infrastructures. Therefore, the other main element of smart mobility is, the intelligent (transport) infrastructure, which will be needed for the usage of autonomous vehicles. For both elements, the safe communication among the components of the system will play a key role in the operation.

Figure 1 shows an example of an autonomous intelligent vehicle's interaction/communication with physical and cyber infrastructures. Today such vehicles also contribute to the totality of a cyber-physical system. Automation - the development of cooperative transport systems and smart mobility - involve the digitalization of the automotive industry. Large-scale automation also aims to reduce the risk of human errors in the process of transportation. However, this development has a price: the effects from using cyber-physical systems must be examined during the development of autonomous intelligent vehicle systems. With the cybernetization of the industry or with the application of machines that are capable of learning, the concept and issues of safety need to be examined from a broader perspective.

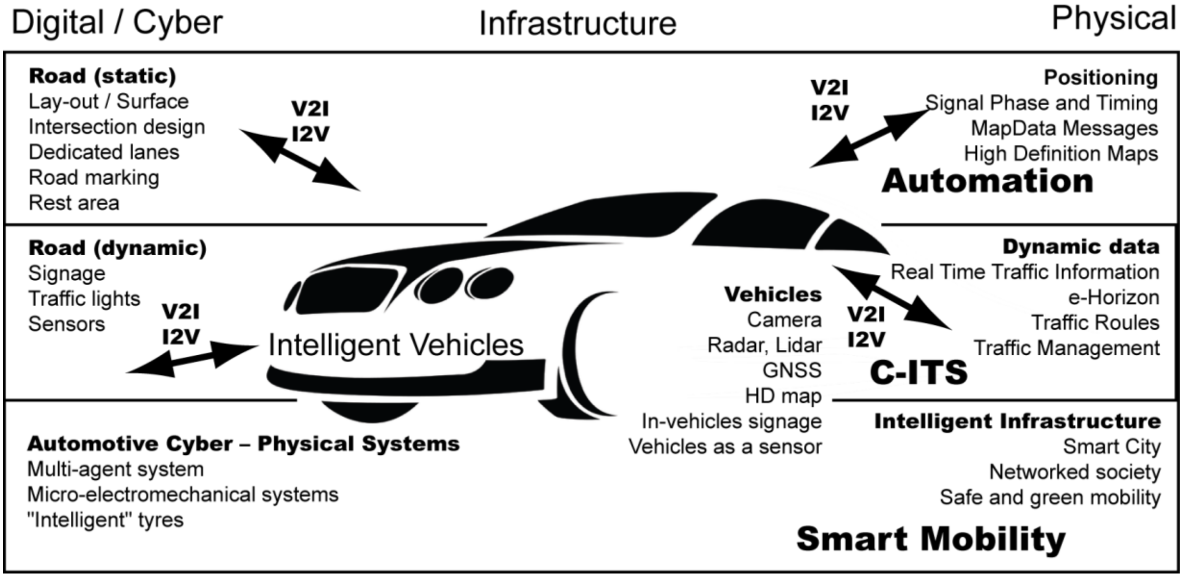

Figure 1. Strategy model of Cyber-Physical Vehicle Systems and Infrastructure (edited from [16]).

The strategy model of cyber-physical vehicle systems and infrastructures represents a plan or model, which aims to improve the safety and security of the transportation process. From the beginning stage of transportation system transformation through the way towards the implementation of cooperative intelligent transportation and smart mobility, smart vehicles will share the road with traditional vehicles – a situation which may last for a long time. In order to achieve smart mobility, besides the concept of vehicle development, research needs to be done during the planning of intelligent transportation systems about the infrastructure of transportation (fast roads, charging lanes, transport hubs, overpasses, etc.). Interactions between intelligent transportation infrastructures and autonomous vehicles need to be planned as well. Vehicle development can involve a number of fields (e.g. vehicular ad hoc network) which may become an infrastructural issue later. The same services and applications required to remain compatible during the long process of the transportation system development, even in the simplest data representation. Therefore, issues with long-term compatibility must receive special attention at the planning of the mobility system.

According to a tentative definition "Intelligent Transport Systems (ITS) are advanced applications which, without embodying intelligence as such, aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated and *smarter* use of transport networks." This definition, however, has become outdated even on a European level. This obviousness can be well illustrated by the relationship between ITS and C-ITS systems: "Vehicles are getting safer, cleaner, and more intelligent. Various sensors and assistant systems enable vehicles to monitor their environment. By means of information exchange among vehicles, as well as between vehicles and the roadside infrastructure, vehicles transform from autonomous systems into cooperative systems. Inter-vehicle communication is a cornerstone of intelligent transportation systems (ITS), commonly referred to as cooperative ITS (C-ITS) or car-2-X communication."

During the planning phrase the strategy that says planning phase that "the focus can no longer be on the infrastructure layer alone (for instance roads and vehicles). Digital technologies also build on a data layer which contains both static data such as digital maps or traffic regulations and dynamic data such as real-time traffic information. These data are then used to develop a layer of innovative services and applications, which are made available over a layer of networks" [17] must be considered as well. This will allow the development of real cooperative intelligent transport systems in Europe with interconnected and automated mobility. C-ITS will provide an interoperable solution at a European level. Due to its insular structure, it cannot be tested in its full functionality; therefore the planning of cooperation is of primary importance. "An integrated transport system relies on the interoperability of its components. That means that systems need to be able to interact with each other, across borders and transport modes, at all levels: infrastructure, data, services, applications and networks." [17]. This interaction can be ensured through communication. "The coordinated and rapid deployment of cooperative, connected and automated vehicles will make an important contribution to improving road safety, increasing the efficiency of road transport, and ensuring the competitiveness of EU industry." [17]. C-ITS does not only refer to road transport. This fact is important to consider at the planning phase, as the development of a smart mobility system will depend on the implementation of the C-ITS.

The sector of transportation is a major energy consumer and emission source. At the planning of the energy efficiency of a smart mobility system, it is not enough to think about the use of renewable energy. It is much more important to provide a plan for cooperation to ensure the operability of the system. For example, congestions or unnecessary waiting times should be reduced in the system. Therefore, it should be possible to ensure the cooperation between the infrastructure and the various vehicles. The energy efficiency of the transportation sector may also depend on the throughput of the system, the fuel consumption and transport capacity of the vehicles, etc. For example, in the course of organizing transportation, various European systems and smart services are available to help the planning of optimal usability, the rationalization of energy consumption in the smart mobility system. In road transportation it is essential to ensure the full coverage of mobile communication, but the infrastructure itself will not become smart only by fulfilling this requirement. In order to develop an intelligent transport system it is not enough to simply introduce WIFI, LED or electric cars, but it is necessary to ensure the overall transformation of the transport infrastructure by the system-level integration of such new technologies as the use of intelligent materials, wireless sensor networks, energy harvesting, etc. The essence of planning an intelligent transport infrastructure lies within its people-oriented approach, which aims to provide maximum services for people by maintaining safety, convenience and sustainability on the long term. One way to achieve this is to make vehicles and infrastructures intelligent. In an intelligent system communication has a prominent role. As its operation is based on communication, the data processing centre of traditional transport monitoring systems needs to be further developed to create a C-ITS. Most probably it is a cloud-base approach which will be applied in intelligent transport systems instead of a centralized monitoring solution. A good example for this is the hybrid smart vehicular ad hoc network.

SERVICES OF SMART MOBILITY

The real contents of smart services have not yet been clearly identified in common practice. The main goal of smart services is to put a user into such a psychological state which helps to accept changes and adopt novelty ideas naturally with regard to various technological innovations. One aspect of the planning of self-driving cars is to provide a comfortable, cosy, relaxing and entertaining experience during the travel. Individual ideas, however, do not make a smart solution without cooperation; therefore it is necessary to make plans for the cooperation of these services. In this sense an " 'ITS service' means the provision of an ITS application through a well-defined organisational and operational framework with the aim of contributing to user safety, efficiency, comfort and/or to facilitate or support transport and travel" [18].

One of the basic requirements of a smart mobility system which must be considered at the planning phase is that through the optimal use of traffic and travelling data it should enable the users of the intelligent infrastructure to plan their routes automatically in accordance with the basic principles of ITS services. In case of the C-ITS services related to passenger and goods traffic, uninterrupted services should be ensured at the crossing of borders in Europe. Thus, the primary goal is to provide real-time traffic information and multimodal travel information services across the EU. It is also important to develop such C-ITS applications which are related to road safety or other protective and preventive measures, e.g. applications which give a warning in case of poor visibility or at the presence of any objects, people or animals on the road. By creating the necessary vehicle-vehicle, vehicle-transport infrastructure and transport infrastructure-vehicle connections to enable safe data and information exchange, these goals can be achieved through automation, based on the data collected by the sensors of autonomous intelligent vehicles.

With regard to intelligent transport infrastructures and their related services, various elements could be identified during the planning phase: smart road, smart parking places, smart energy supply points, which may have an important role on the level of services in the development of a smart mobility system. The main criteria of a smart road that is should fit into the existing infrastructure and it should support both individual and community transport. Intelligent infrastructure creates safety and in case of a danger, it ensures prompt counter-measures. The provision of information and booking services regarding safe and protected parking places is also part of the development of smart mobility systems. In case of parking or rest areas, intelligent street lighting, surveillance and security camera systems allow further automation in operation.

Concerning the development of parking or accommodation booking systems, further research needs to be done in tourism and in user experience. On-road accommodation may be offered for those people who travel across several countries. However, those who travel to specific destinations will not opt for roadside motels if they can find accommodation with a higher service level nearby. On the level of services, it must be examined how such real-time information about local opportunities can be sent to passengers during the time of travelling. The provision of online real-time data/information on regional transfer points and empty or free parking places raises similar questions. Occupancy forecasts may not only be made on the basis of the information about free places or by other data of the booking system, but by the self-diagnoses of vehicles, through which it can be predicted which vehicle will need to stop (at the beginning stage, at the presence of a driver, he can be alerted in advance). This stopover may be calculated from the state of charge of the vehicle's battery, or it is possible to alert to any necessary servicing. The vehicle may book a parking place automatically, if it knows what parameters it has.

In the absence of self-driving cars, or in the transitional period, an application could be introduced to check the drivers' alertness and their capability to drive, and to warn them or, as an embedded solution, to stop the vehicle for an imposed rest. In case of the use of self-driving cars, the use of roadside rest areas will become less relevant. In a fully automated system, there is no need to wait for a driver to regain his alertness, while in a hybrid transport system, where self-driving and traditional vehicles are both present, this is still necessary to ensure. In order to enhance the services of rest areas it is important to examine user demands with regard to eating and other physical needs.

In a smart mobility system a number of services can be offered to support the use of alternative fuels. In the case of e-mobility, a major task is to connect and integrate the vehicles into the electric energy system, and a wide range of smart solutions could be developed for this purpose. Until the use of electric transport becomes everyday practice, it is important to provide prompt and adequate information for the users about the application of these new technologies. There are various IT-based solutions to provide such services. Sustainable transportation may not only be approached from the point of energy efficiency. For example, automated waste collection in parking and rest areas should also be resolved. In the future, the automated collection of dropped litter or the remote monitoring of the fullness of waste bins and their automated emptying may be realized by the use of mobile robots integrated into the smart mobility system, among other elements of the infrastructure maintenance service.

THE CONCEPT OF SAFETY AND SECURITY IN AUTONOMOUS INTELLIGENT CYBER-PHYSICAL VEHICLE SYSTEMS

In order to reduce the complexity and increase the flexibility of electric cabling in motor vehicles a bus system has been implemented. With a growing scope of functionalities, the number and variety of bus systems have increased. The buses of safety functions have been separated from the networks ensuring convenience functions. Nevertheless, experience has shown that a significant proportion of motor vehicles in traffic can be affected by the vulnerability of networks from the point of cyber security. Convenience functions are not always given adequate protection and some functions are implemented without any protection at all. These security gaps can be used to access certain security functions, to disrupt their operation or take over their control even without a direct physical connection. Therefore, at the planning of autonomous intelligent vehicles, the main elements of the smart mobility system, these cyber security issues must also be considered.

SAFETY OF AUTONOMOUS INTELLIGENT CYBER-PHYSICAL VEHICLE SYSTEMS

With regard to autonomous intelligent vehicles, safety means that a given vehicle must be kept in such a condition which ensures the highest level of protection of human lives. “Safety describes the effort to prevent mistakes in the core functions of a vehicle or, in a worst case, to protect the occupants and other persons involved from harm. Components such as brakes, steering, airbags, and the crumple zone of a car, but also electronic assistants such as ESP or ABS are critical to safety” [19]. Land vehicles are important elements of intelligent transport systems. At the planning or checking of the safety of autonomous intelligent land vehicles, the following aspects defined by SAE International are considered: functional safety, active safety (e.g. Advanced Driver Assistance System), safety and reliability (e.g. electronics and electrical systems; hardware and software verification and validation [20]), safety and human factors.

Figure 2 shows an example of the cyber-physical systems related to the road safety of autonomous intelligent vehicles together with the systems related to the vehicle’s environment. As it is well illustrated by this example, the information, warning, control, intervention, severity reduction or rescue systems, which actively or passively ensure the road safety of vehicles, should all be considered from the aspect of cyber security.

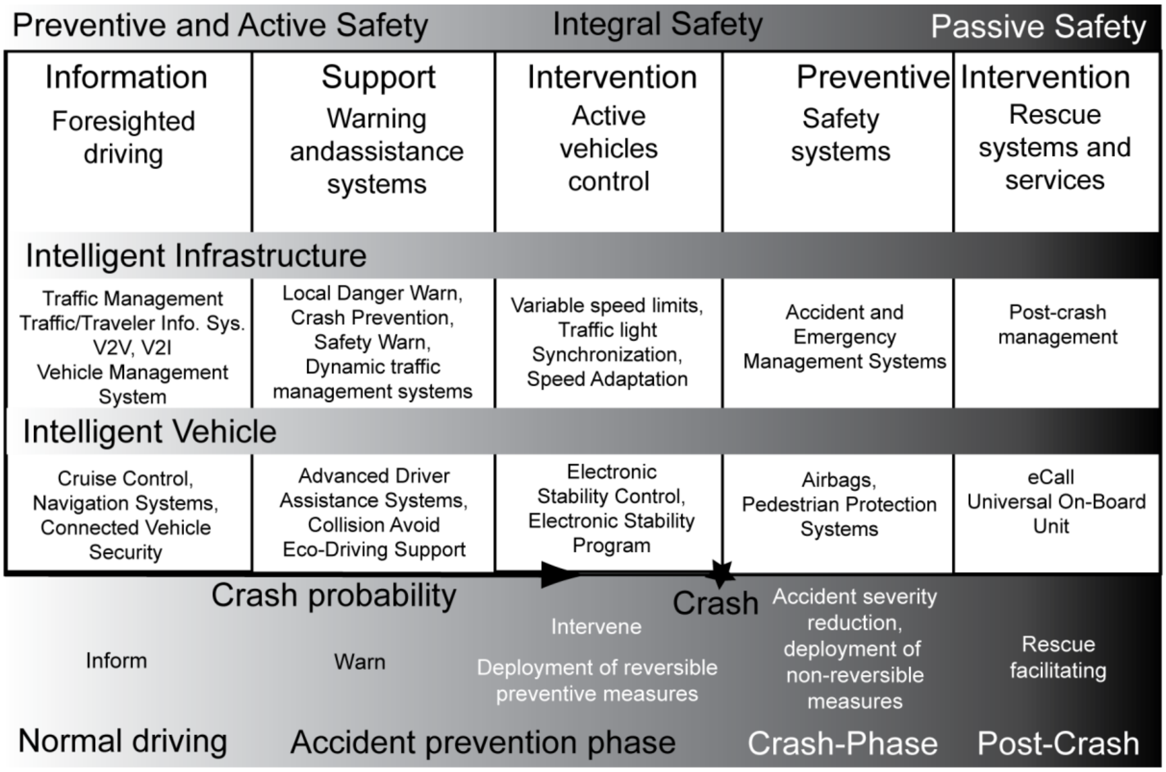
Preventive and Active Safety
Integral Safety
Passive Safety
Information
Foresighted driving
Support
Warning andassistance systems
Intervention
Active vehicles control
Preventive
Safety systems
Intervention
Rescue systems and services
Intelligent Infrastructure
Traffic Management
Traffic/Traveler Info. Sys.
V2V, V2I
Vehicle Management System
Local Danger Warn,
Crash Prevention,
Safety Warn,
Dynamic traffic management systems
Variable speed limits,
Traffic light Synchronization,
Speed Adaptation
Accident and Emergency Management Systems
Post-crash management
Intelligent Vehicle
Cruise Control,
Navigation Systems,
Connected Vehicle Security
Advanced Driver Assistance Systems,
Collision Avoid
Eco-Driving Support
Electronic Stability Control,
Electronic Stability Program
Airbags,
Pedestrian Protection Systems
eCall
Universal On-Board Unit
Crash probability
Crash
Inform
Warn
Intervene
Deployment of reversible preventive measures
Accident severity reduction, deployment of non-reversible measures
Rescue facilitating
Normal driving
Accident prevention phase
Crash-Phase
Post-Crash

Figure 2. Safety phases of the Autonomous Intelligent Cyber-Physical Vehicle Systems (edited from [16, 21]).

“Safety integrity refers to the likelihood of a safety related system satisfactorily performing the required safety functions under all the stated conditions, within a stated period of time: without any unsafe failures. The Safety Integrity Level (SIL) assigned to a system determines the development, planning, manufacturing and operating methods that should be applied.” [22]. According to certain classifications, three areas of safety can be distinguished: functional safety, technical safety and contextual safety (EN 50126-2:2017). In case of safety critical systems in the auto-industry, the values of ASIL (Automotive Safety Integrity Level) are used throughout the lifecycle of vehicles.

SECURITY OF AUTONOMOUS INTELLIGENT CYBER-PHYSICAL VEHICLE SYSTEMS

Security means the provisions made to ensure the protection of property against theft. One example for this is the way the money stored in ATMs is protected, or the use of passwords or data security in information technology. Therefore, at the checking and planning of autonomous intelligent land vehicles from the point of security the primary aim is to build a cyber safe system. With regard to the vehicles, vehicle systems and intelligent infrastucture within the intelligent transport system, other aspects of security have also been identified in the present research. “Security, on the other hand, means the security of software systems against malfunctions and external attacks. Software in cars has various roles: engine control, external communications, but also car safety and security.” [19]. In the transport system, the digits ‘1201012356’ for example, can be used as some data. If such data, however, represent the communication ID of a vehicle in the ad hoc network of vehicles, it will also represent some information within the system. According to Muha, in the taxonomy of information security, the circle of elements to be protected include the persons, the physical environment of the system, the infrastructure necessary for operation, the hardware and software products, communication devices and networks, data carriers and regulations [23].

Information security focuses on the confidentiality, integrity and availability of information. In addition, cyber security means the protection of infocommunication systems. As it can be seen in Figure 3, cyber security includes everything and everyone that can access the applications of the vehicle industry through the cyber space.

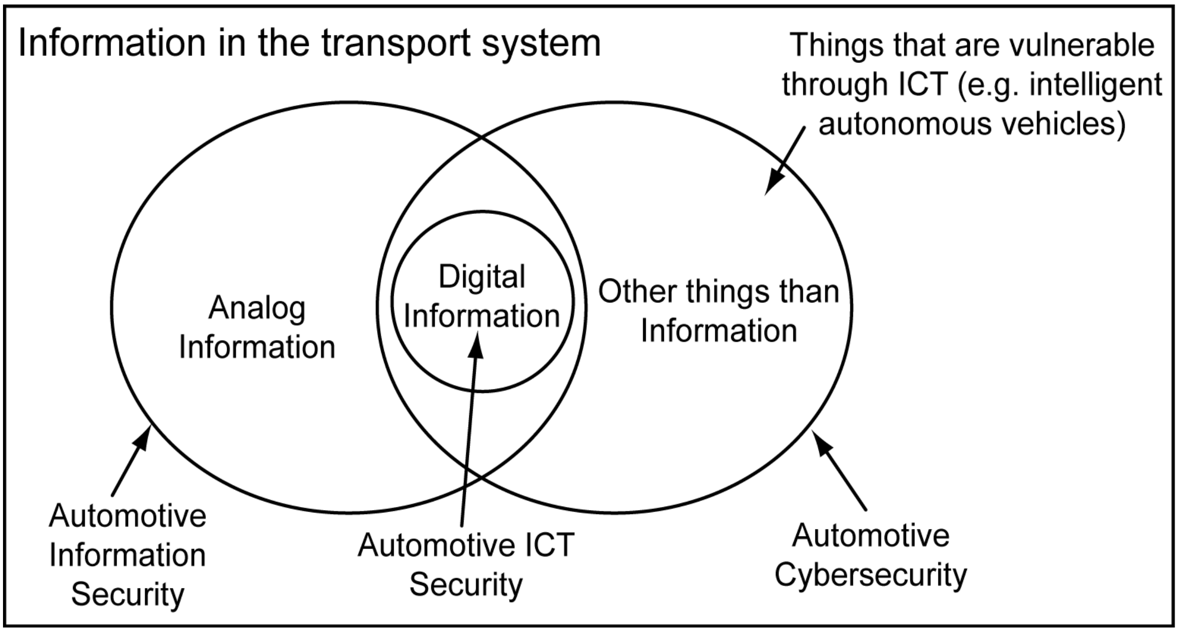
Information in the transport system
Things that are vulnerable through ICT (e.g. intelligent autonomous vehicles)
Analog Information
Digital Information
Other things than Information
Automotive Information Security
Automotive ICT Security
Automotive Cybersecurity

Figure 3. Venn diagram of the difference between Automotive Cyber security and Automotive Information Security [24] (authors' edit).

SAFETY AND SECURITY THROUGH ITERATIVE DESIGN – VEHICLES CYBERSECURITY SYSTEMS ENGINEERING, RISK-ORIENTED DEVELOPMENT

Figure 4 shows the iterative development process of smart mobility ecosystems. The safety and security-related development of the two basic elements of smart mobility must follow this process. The process of safety and security development is also represented in Figure 5.

The automotive connected world poses threats to product safety and performance, data integrity and access, privacy and interoperability. The ISO 26262 standard on the functional safety of the electronic systems of road vehicles already provides rules and planning guidelines, while Edition 2 specifies the requirements of cyber security procedures for interfaces. Nevertheless, this field still needs an overall automotive-specific cyber security standard. The relevant cyber security ISO standard is at the proposal stage, while the SAE standard is currently being developed, but the first edition of the recommended practice J3061TM was already issued in January 2016. Of course, other standards also affect automotive developments in the cyber security engineering process, including some general IT security standards (ISO 27001, ISO 15408) or specific security standards for V2X communications (IEEE 1609.2, ETSI TR 102 638 V1.1.1).

As this field is still in its infancy, automotive cyber security engineering processes are yet to be developed in accordance with the related standards and best practices (SEA – Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061). Cyber security engineering processes must comply with the existing systems of functional security and quality processes, and the adequately qualified personnel should be able to perform these security. The IEC 62443 standard defines four security levels, including qualitative indicators, competences and effort levels for a successful attack against the system.

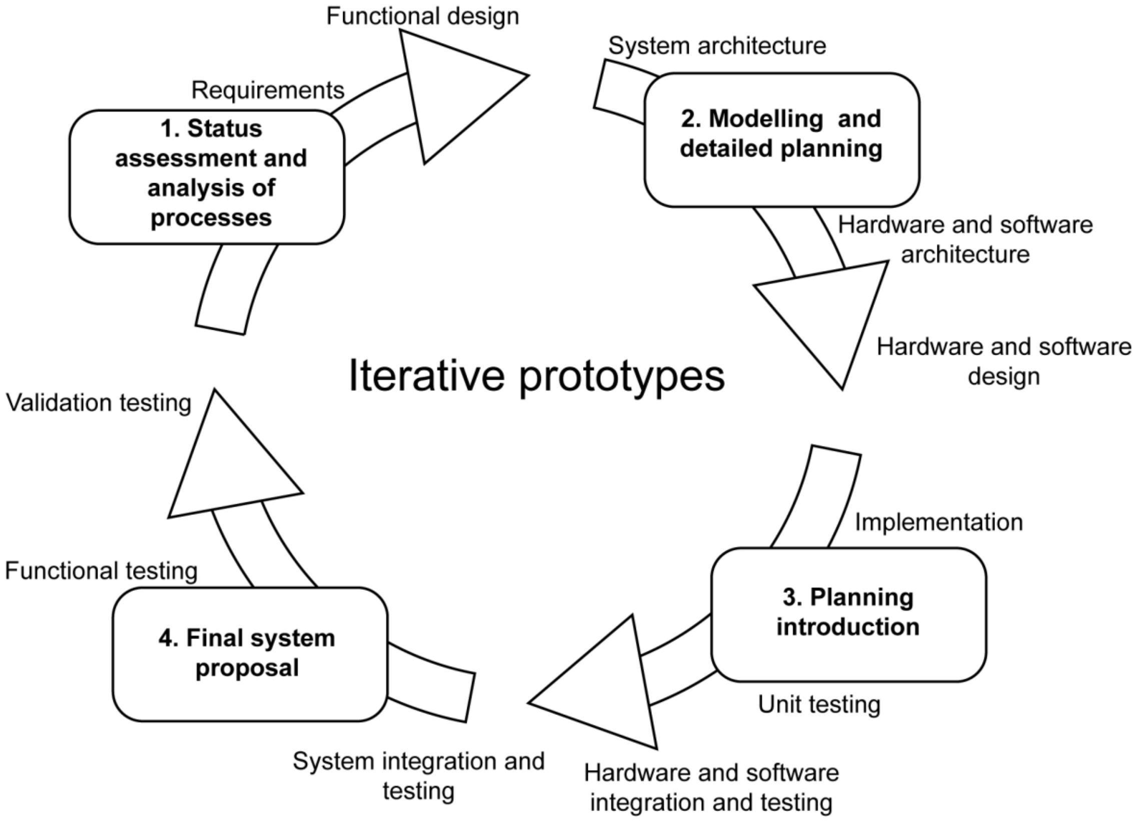
Functional design
System architecture
Requirements
1. Status assessment and analysis of processes
2. Modelling and detailed planning
Hardware and software architecture
Hardware and software design
Iterative prototypes
Validation testing
Implementation
Functional testing
3. Planning introduction
4. Final system proposal
Unit testing
System integration and testing
Hardware and software integration and testing

Figure 4. The development process of the iterative prototypes of smart mobility ecosystems [16] (authors' edit).

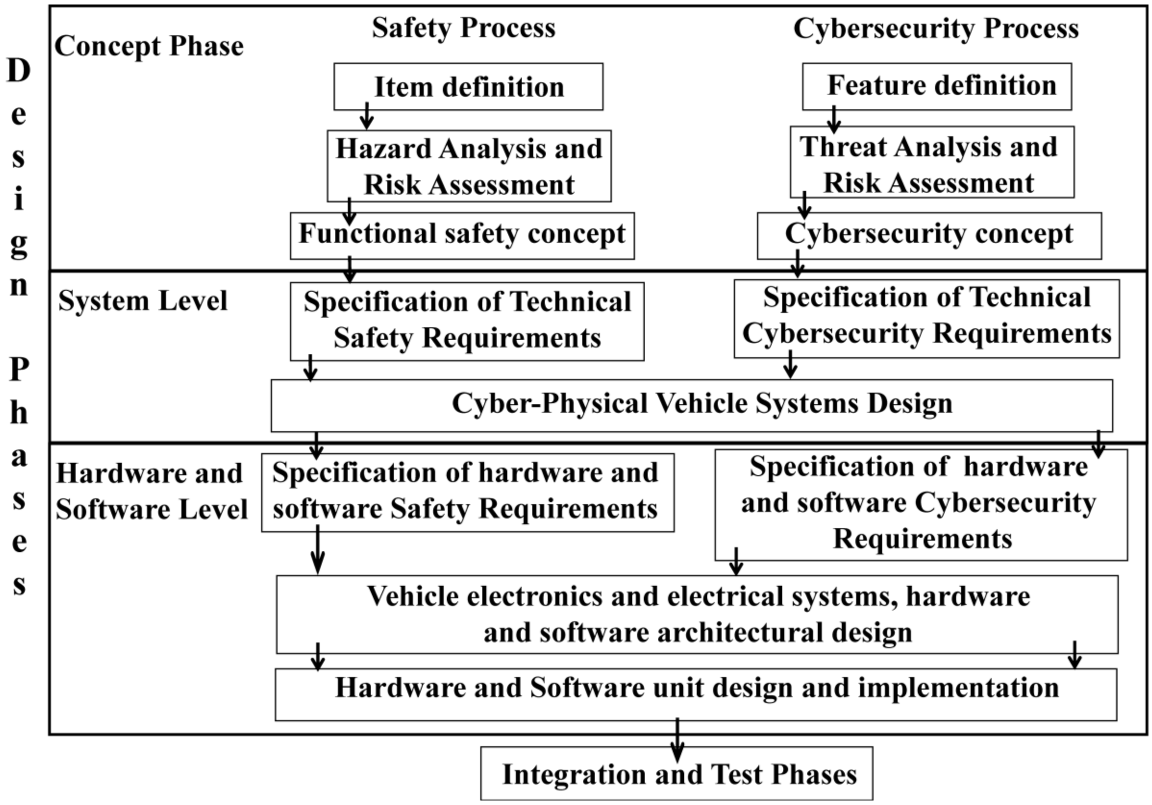
Design Phases
Concept Phase
Safety Process
Cybersecurity Process
Item definition
Feature definition
Hazard Analysis and Risk Assessment
Threat Analysis and Risk Assessment
Functional safety concept
Cybersecurity concept
System Level
Specification of Technical Safety Requirements
Specification of Technical Cybersecurity Requirements
Cyber-Physical Vehicle Systems Design
Hardware and Software Level
Specification of hardware and software Safety Requirements
Specification of hardware and software Cybersecurity Requirements
Vehicle electronics and electrical systems, hardware and software architectural design
Hardware and Software unit design and implementation
Integration and Test Phases

Figure 5. Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure [25, 26] (authors' edit).

In the course of the development process, functional safety as well as cyber security, hazard analysis and risk assessment as well as threat analysis and risk assessment, safety concepts and requirements as well as security concepts and requirements, system design as well as defence-in-depth system planning must all be conducted as shown in Figure 5. Cyber security should not simply be an additional element of the development process, but it should make an integral part of the planning phase, from the conceptual stage, through the manufacturing, operation and servicing to the decommissioning of the system. This is what the overall lifecycle management of cyber security means and it is realized in the course of the cyber security engineering process [22]. The automotive cyber security integrity level of the developed electrical, electronic and programmable electronic safety-related systems can be defined with the relevant ACSIL (Automotive Cyber Security Integrity Level) values.

CONCLUSIONS

According to Cohen, one of the main elements of the smart city is smart mobility[27]. The present article discussed the design process of this new mobility system. As the research pointed out, the two main elements of smart mobility are autonomous intelligent vehicles and vehicles systems, and intelligent transport infrastructures. The development of smart mobility has become necessary with the demand for creating cooperative intelligent transport systems. These endeavours aim to increase productivity (transport capacity, comfort), to reduce the number of accidents or the emission of harmful materials in city transport. Smart city transport can be conceived as an advanced ITS system. The marketing of smart city mobility focuses on the provision of additional services which are not available in traditional systems. The present article has shown a number of smart mobility solutions. The use of autonomous intelligent vehicles is becoming increasingly widespread (robots [28], drones [29] and self-driving cars [30]) due to their overall benefits on the society [31]. Today's advanced robot systems [32], such as self-driving cars, are capable of platooning or reaching a selected destination autonomously. Besides vehicle-to-vehicle communication, V2X (Vehicle-to-everything) communication must also be ensured to create a smart city. The functional and operational safety of vehicles has long been researched, but besides the physical infrastructure and the physical systems of the vehicles, cyber-physical complex systems are playing an increasingly important role. The cyber-security approach of automotive developments is a new but fast developing field. The present article described the aspects of the safety and cyber security-related planning of electrical, electronic and programmable electronic safety-related systems in the development of smart mobility [33].

ACKNOWLEDGEMENT

The research presented in this article was carried out as part of the project in the framework of the New Széchenyi Plan, No. EFOP-3.6.2-16-2017-00016. The completion of this project is funded by the European Union and co-financed by the European Social Fund.

REFERENCES

[1] Steinbaeck, J.; Steger, C.; Holweg, G. and Druml, N.: *Next generation radar sensors in automotive sensor fusion systems*.
2017 Sensor Data Fusion: Trends, Solutions, Applications. IEEE, Bonn, pp.1-6, 2017, http://dx.doi.org/10.1109/SDF.2017.8126389,

[2] Liubakka, M.K.; Rhode, D.S.; Winkelman, J.R. and Kokotovic, P.V.: *Adaptive automotive speed control*.
IEEE Transactions on Automatic Control **38**(7), 1011-1020, 1993, http://dx.doi.org/10.1109/9.231457,

[3] Park, S.H. and Lee, S.Y.: *Development of On-board Diagnosis via CAN for a HVI (Human Vehicle Interface) Technology*.
2012 IEEE 10th International Symposium on Parallel and Distributed Processing with Applications, 10-13 July, 2012. IEEE, Leganes, 2012,
http://dx.doi.org/10.1109/ISPA.2012.125,

[4] Stepanic, J.; Mester, G. and Kasac, J.: *Synthetic Inertial Navigation Systems: Case Study of Determining Direction*.
Proceedings of the 57th ETRAN Conference, Society for Electronics, Telecommunications, Computers, Automatic Control and Nuclear Engineering. Zlatibor, pp.RO2.7.1-RO2.7.3, 2012,

[5] Albini, A. and Rajnai, Z.: *General Architecture of Cloud*.
Procedia Manufacturing **22**, 485-490, 2018,

[6] Chaxel, F.; Bajic, E. and Richard, J.: *Automotive vehicle data management based on holon-product paradigm*.
Systems, Man, and Cybernetics. IEEE SMC, Tokyo, 2002,
http://dx.doi.org/10.1109/ICSMC.1999.816591,

[7] Walch, M., et al.: *From Car-Driver-Handovers to Cooperative Interfaces: Visions for Driver-Vehicle Interaction in Automated Driving*.
In: Meixner, G. and Müller, C., eds.: *Automotive User Interfaces: Creating Interactive Experiences in the Car*. Springer International Publishing, 2017,

[8] Waschl, H.; Kolmanovsky, I.; Steinbuch, M. and del Re, L., eds.: *Optimization and Optimal Control in Automotive Systems*.
Springer International Publishing, 2014,
http://dx.doi.org/10.1007/978-3-319-05371-4,

[9] Sarker, A.; Qiu, C. and Shen, H.: *Quick and Autonomous Platoon Maintenance in Vehicle Dynamics for Distributed Vehicle Platoon Networks*.
2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, Pittsburgh, 2017,

[10] Oraibi, I.; Otero, C.E. and Olasupo, T.O.: *Empirical path loss model for vehicle-to-vehicle IoT device communication in fleet management*.
16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net). IEEE, Budva, 2017,
http://dx.doi.org/10.1109/MedHocNet.2017.8001659,

[11] Chisalita, L. and Shahmehri, N.: *A peer-to-peer approach to vehicular communication for the support of traffic safety applications*.
The IEEE 5th International Conference on Intelligent Transportation Systems. IEEE, Singapore, 2003,
http://dx.doi.org/10.1109/ITSC.2002.1041239,

[12] Krodel, M. and Kuhnert, K.D.: *Towards a learning autonomous driver system*.
26th Annual Conference of the IEEE Industrial Electronics Society. IECON 2000. 2000 IEEE International Conference on Industrial Electronics, Control and Instrumentation. 21st Century Technologies. IEEE, Nagoya, 2002,
http://dx.doi.org/10.1109/IECON.2000.973125,

[13] Iantovics, L.B., et al.: *Review of Recent Trends in Measuring the Computing Systems Intelligence*.
Broad Research in Artificial Intelligence and Neuroscience **9**(2), 77-94, 2018,

[14] Iantovics, L.B.; Emmert-Streib, F. and Arik, S.: *MetrIntMeas a novel metric for measuring the intelligence of a swarm of cooperating agents*.
Cognitive Systems Research **45**, 17-29, 2017,
http://dx.doi.org/10.1016/j.cogsys.2017.04.006,

[15] Özkul, M. and Çapuni, I.: *An autonomous driving framework with self-configurable vehicle clusters*.
2014 International Conference on Connected Vehicles and Expo. IEEE, Vienna, 2015,
http://dx.doi.org/10.1109/ICCVE.2014.7297590,

[16] European Commission: *C-ITS Platform Phase 2.* https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf, accessed 8th March 2018,

[17] European Commission: *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, conn.* https://ec.europa.eu/energy/sites/ener/files/documents/1_en_act_part1_v5.pdf, accessed 8th March 2018,

[18] European Parlament: *Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport*. Official Journal of the European Union, 1-13, 2010,

[19] Deloitte GmbH: *Automotive Software Quality What do OEM's have to consider for the future?* https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Risk-Risk-Advisory-Automotive-Software-Quality-EN-s.pdf, accessed 8th March 2018,

[20] Schuster, G.; Tokody, D. and Mezei, I.J.: *Software Reliability of Complex Systems Focus for Intelligent Vehicles*. In: Jármai, K. and Bolló, B., eds.: *Lecture Notes in Mechanical Engineering – Vehicle and Automotive Engineering*. Springer, Heidelberg & Miskolc, 2017, http://dx.doi.org/10.1007/978-3-319-51189-4_28,

[21] Safety Forum: *Final Report and Recommendations of the Intelligent Infrastructure Working Group.* http://www.apcap.pt/downloads/Intelligent_Infrastructure_Report_v1_0_20101012.pdf, accessed 8th March 2018,

[22] Abonyi, J. and Fülep, T.: *Safety critical systems*. http://moodle.autolab.uni-pannon.hu/Mecha_tananyag/biztonsagkritikus_rendszerek/ch03.html, accessed 8th March 2018,

[23] Muha, L.: *System Theory for Information Security.* Bolyai Szlemle **17**(4), 137-156, 2004,

[24] Ciso platform: *Understanding difference between Cyber Security and Information Security.* http://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information, accessed 8th March 2018,

[25] Ardila, J.P.C. and Gallina, B.: *Towards Efficiently Checking Compliance Against Automotive Security and Safety Standards.* 2017 IEEE International Symposium on Software Reliability Engineering Workshops. IEEE, Toulouse, 2017, http://dx.doi.org/10.1109/ISSREW.2017.33,

[26] Schmittner, C.; Ma, Z.; Reyes, C.; Dillinger, O. and Puschner, P.: *Using SAE J3061 for automotive security requirement engineering*. In: Skavhaug, A.; Guiochet, J.; Schoitsch, E. and Bitsch, F., eds.: *Computer Safety, Reliability, and Security*. Lecture Notes in Computer Science. Springer, Cham, 2016, http://dx.doi.org/10.1007/978-3-319-45480-1_13,

[27] Tokody, D. and Schuster, G.: *Driving Forces Behind Smart City Implementations – The Next Smart Revolution*. Journal of Emerging Research and Solutions in ICT **1**(2), 1-16, 2016,

[28] Mester, G. and Aleksandar, R.: *Sensor-Based Intelligent Mobile Robot Navigation in Unknown Environments.* International Journal of Electrical and Computer Engineering Systems **1**(2), 1-8, 2010,

[29] Rodić, A.; Mester, G. and Stojković, I.: *Qualitative Evaluation of Flight Controller Performances for Autonomous Quadrotors*.
In: Pap, E., ed.: *Intelligent Systems: Models and Applications*. Topics in Intelligent Engineering and Informatics 3. Springer-Verlag, Berlin & Heidelberg, pp.115-134, 2013,

[30] Mester, G.: *Autonomous self-driving robot cars*.
https://www.researchgate.net/publication/324089063_Autonom_onvezeto_robot_autok, accessed 8th March 2018,

[31] Stepanić, J.; Sabol, G. and Žebec, M. S.: *Describing social systems using social free energy and social entropy*.
Kybernetes **34**(6), 857-868, 2005,

[32] Mester, G.: *Obstacle – Slope avoidance and velocity control of wheeled mobile robots using fuzzy reasoning*.
2009 International Conference on Intelligent Engineering Systems. IEEE, Barbados, 2009, http://dx.doi.org/10.1109/INES.2009.4924770,

[33] Tokody, D.; Mezei, I. J. and Schuster, G.: *An overview of autonomous intelligent vehicle systems*.
In: Jármai, K. and Bolló, B., eds.: *Lecture Notes in Mechanical Engineering – Vehicle and Automotive Engineering*. Springer, Heidelberg & Miskolc, 2017,
http://dx.doi.org/10.1007/978-3-319-51189-4_27.