https://doi.org/10.3311/PPtr.15850

Periodica Polytechnica Transportation Engineering, 48(4), pp. 349–356, 2020

Introducing Safety and Security Co-engineering Related Research Orientations in the Field of Automotive Security

Árpád Török[1*], Zsombor Pethő[1]

[1] Department of Automotive Technologies, Faculty of Transportation Engineering and Vehicle Engineering, Budapest University of Technology and Economics, H-1521 Budapest, P. O. B. 91, Hungary
[*] Corresponding author, e-mail: arpad.torok@auto.bme.hu

Received: 03 March 2020, Accepted: 11 March 2020, Published online: 07 August 2020

Abstract

Since modern vehicles are connected and their transport processes are strongly supported by different automated functions, malicious external interventions can impair safety integrity. Therefore, it seems to be reasonable in the future to introduce safety and security co-engineering approaches in the automotive industry. With regard to the performed evaluation, three main promising research orientations have been identified. Automotive safety and security related development of co-engineering methodology and validation framework are of key importance from the viewpoint of autonomous transportation. Accordingly, a scenario based, integrated evaluation of automotive safety and security would be closely fit to the concept of SOTIF and the SoS approach. Beyond this, the communication and network security of "vehicle to everything" channels have to also be in the focus of automotive researches. Additionally, the development of automotive anomaly detection systems, especially focusing on the complex SoS operation processes will be a highly important research orientation.

Keywords

automotive safety, automotive security, safety co-engineering, security co-engineering

1 Introduction

Safety and Security Research Group of the Department of Automotive Technology at Budapest University of Technology and Economics focuses on the latest technological challenges of the automotive sector caused by the strong interactions of safety and security related threats and menaces (Koschuch et al., 2019).

Since modern vehicles are connected and their transport processes are strongly supported by different automated functions, malicious external interventions can impair safety integrity.

Therefore, it seems to be reasonable in the future to introduce safety and security co-engineering approaches in the automotive industry.

In light of the introduced aspects, the current article aims to identify the most relevant research orientation in the field of automotive security. On the other hand, it is also necessary to consider safety related aspects during the identification of the most relevant security issues, since the expected safety effect of a security incident can strongly influence its severity.

In accordance with the presented approach, in Section 2, the most important safety related automotive functions and their evolution are going to be presented.

Then, it is going to be followed by the introduction of the relevant security fields in the automotive sector, especially focusing on technologies, which are expected to have the most significant impact on automotive safety.

Afterwards, Section 2 is followed by the essential part of the paper, which is going to summarize the identified research filed briefly, being expected to have the most significant influence on the field of safety and security co-engineering.

In the final phase of the paper, the achieved results and the most important findings are going to be concluded briefly.

2 Evolution of safety related functions in road transportation

When safety related transport functions are evaluated it seems to be reasonable to start with traffic control system, since this is still one of the most important

Cite this article as: Török, Á., Pethő, Zs. (2020) "Introducing Safety and Security Co-engineering Related Research Orientations in the Field of Automotive Security", Periodica Polytechnica Transportation Engineering, 48(4), pp. 349–356. https://doi.org/10.3311/PPtr.15850

component system of the road transportation systems (Poletan Jugović et al., 2019). Based on the reviewed literature the first traffic signal system was placed into service in 1914 in Ohio (McShane, 1999).

From a safety point of view the year 1960 is also very important, since this is the year when the first dynamic message sign was installed (Roads&Bridges, 2011). At that time, the main objective of the dynamic message signs was to call drivers' attention for dangerous sections of the road network. One of the most common messages was the "reduce speed" sign.

Nowadays, when the field of automated safety functions are investigated in the field of road transportation, it is important to emphasize the role and importance of navigation systems. If the most significant evolution milestone of navigation systems should be highlighted, many experts would primarily emphasize the relevance of TRANSIT navigation system. The TRANSIT system was developed in 1960 and it provided estimated location data based on the information of five satellites (Black, 1990). In the next decades, Global Navigation Satellite Systems (GNSS) made it possible to apply real time localization and navigation in transportation. In the automotive sector, the possibility a higher accuracy localization for civilian application became available in the last decade of the twentieth century, which penned the gates even for safety applications.

To continue introducing the evolution of safety functions in vehicle systems the development of brakes have to be reviewed. The first brakes applied the same physical principles as today's brakes, however the components were completely different. The first construction which was already similar to currently applied systems was invented by Gottlieb Daimler and further developed by Louis Renault in 1902 (Abeysiriwardhana and Abeykoon, 2014). From this level, the evolution of brakes arrived to the market ready Anti-lock Braking Systems (ABS) in the 1970s, when Robert Bosch started to perform comprehensive research activity in this field (Schinkel and Hunt, 2002). Later the theory of Electronic Stability Program (ESP) modules from the 1990s was significantly based on the operation process of ABS (Liebemann et al., 2004). Nowadays, the operation processes of latest generation vehicular control systems are in a strong cooperation with the highly safety critical braking function, contributing to the dynamic stability of the vehicles' motion as well. There is a strong relationship among developed braking functionalities and other advanced driver assistance systems like:

- Adaptive Cruise Control (ACC) introduced by Mitshubishi in 1992 (Xiao and Gao, 2010),
- Intelligent Parking Assist Systems (IPAS), developed by Toyota, 1999 (Vestri et al., 2005),
- Lane Keeping Assist Systems (LKS) introduced by Nissan in 2001, (Amditis et al., 2010),
- Lane Change Assist Systems and Blind Spot Monitoring Systems, introduced by Volvo in 2007,
- Collision Avoidance Systems (CAS) introduced by Toyota/Volvo in 2008 (Sari et al., 2017),
- mandatory deployment of automotive emergency call service (eCall) devices in new cars in the EU, 2018 (Oorni and Goulart, 2017),
- deployment of standardized V2X communication unit, introduced by Toyota from 2015, Volkswagen from 2019 (Renner et al., 2020).

To sum up the evolution of safety related functions in road transportation, it can be concluded that safety related functions can be classified in three relevant groups.

First system group contains the infrastructure related solutions especially considering traffic control and traffic management systems.

Beside this, vehicle related systems constitute another separated research field.

Furthermore, as it has been learnt from the review of system evolution processes, in case of the most up-to-date systems, communication based safety solutions started to play an outstandingly important role in the transportation sector.

According to the expectations of the scientific society (Nadezda et al., 2017), future transportation systems will provide the required safety level through the cooperative application of the aforementioned system groups. In light of this, effective, reliable and aligned cooperation of these system components is one of the most crucial challenges of future autonomous transportation systems (Zöldy, 2019).

The complexity of these cooperative systems makes it necessary to introduce new approaches in developing, providing, testing and validating the safety of these systems.

Those newly developed safety concepts (methods and models), which contribute to completing the safety requirements of complex automated transportation systems are collectively referred as system of systems concept (Koschuch et al., 2019).

3 Introduction of security related issues in road transportation

In the first part of the twentieth century, transportation security related issues focused primarily on the protection of vehicle property and critical infrastructure. In case of road transportation, this field covered the vehicle

alarm systems, immobilizers, and physical lock modules. Especially focusing on road transportation, security related challenges mainly occurred related to the field of unauthorized usage, and in some cases - related to malicious interventions focusing on data recording devices (e.g. odometers or commercial vehicle tachographs).

This situation was fundamentally changed, when the appearance of programmable hardware devices, widely known as key fobs made it possible to have physical access to vehicles without physical connection.

At the same time, vehicles started to be equipped by dozens of Electronic Control Units (ECU). On the one hand, this made it possible to improve the level of safety, efficiency, emission and performance of road transportation; however, on the other hand the vulnerability of vehicles was significantly increased. Especially, when vehicle maintenance related issues made it necessary to provide access to the in vehicle communication network through a diagnostic port, the vulnerability of the vehicular communication system was dramatically grown. The impact of this trend on vehicle safety became more and more relevant due to the permanently increasing number of in-built ECUs. Therefore vehicles started to transform from a mainly mechanical construction to the cooperative system of electronic controllers. In these systems, the operation efficiency of the vehicle is strongly influenced by the characteristic of the in-built information technology system modules, which are responsible for the safe and reliable data transfer processes (Navet and Simonot-Lion, 2013).

To improve the protection of the vehicular systems, numerous sector-specific solutions were applied by the automobile sector. To reduce the vulnerability of keyless fobs some manufacturer produced models with ultra-wide-band radio technology, which makes it considerably more challenging for perpetrators to play back the signal. Beside this, more and more producers introduce keyless fobs with automatically and manually adjustable sleeping mode.

On the other hand, in case of many models, some safety critical segments of the In Vehicle Networks (IVN) are still not protected by encryption, which is still a significant vulnerability of road vehicles.

Beyond the less visible and less accessible segments of IVN, most of the currently purchasable cars have complex on-board head-units with highly developed functionalities covering a wide range of offline and online multimedia services. These systems are temporary or permanently connected either to a restricted network or to the cyberspace. Similarly to IVNs, the complex connectivity can be identified as a new emphatic characteristic of future Inter-Vehicular Communication (IVC) systems. Due to this complex connectivity of IVC systems, it does not seem to be a simple challenge to supervise and secure future transportation processes. Especially, when the expected system vulnerabilities of the Vehicular Ad-hoc Network (VANET) concept are considered.

In accordance with this, nowadays, the perpetrators of malicious interventions can go much further than a vehicle theft. Personal data or private information stored or generated (e.g. behavior of the user, spatial characteristic of user motion) in the vehicle can be theft remotely, control over the vehicle can be taken from the cyberspace and safety critical vehicle modules can be influenced through digital communication channels.

Therefore, in the last few years, the importance of automotive security became obvious for manufacturer. There are some important initiatives, which focus on the treatment of security related challenges in the automotive industry. AUTomotive Open System ARchitecture (AUTOSAR) is a worldwide cooperation of actors from the automobile industry. The most important aim of the cooperation is to identify a freely available and interoperable software framework for vehicle ECUs. Beside this, it is important to emphasize that AUTOSAR pays particular attention to automotive cybersecurity (Kandimala and Sojka, 2012).

Moreover, there are some sector specific initiatives, which directly focus on automotive security related methodologies. E-safety Vehicle Intrusion Protected Applications (EVITA). The purpose of EVITA is to design, validate, and demonstrate a framework focusing on automobile IVNs, especially considering the security of those ECUs, which play a key role in the operation processes of the vehicle (Nilsson et al., 2008).

The main objective of SEIS (Sicherheit in eingebetteten IP-basierten Systemen / Security in embedded IP-based Systems) project is to evaluate the applicability of the Internet Protocol (IP) in case of vehicular communication, especially considering the occurring security related challenges.

Based on the performed literature review, the evolution of vehicular security can be summarized as follows:

- first automotive ECU introduced by Volkswagen AG, in 1968 (Ullrich, 2015),
- first remote keyless entry system introduced by Ford, in 1980 (Rivard, 1980),
- mandatory OBD port deployment introduced in California, in 1991 (Tahat et al., 2012),
- first deployment of a central gateway, introduced by BMW, in the period of 2004–2008 (Matheus and Königseder, 2017),

- first proposal for automotive HoneyPot security concept for IVN, in 2008 (Verendel et al., 2008),
- first proposal for anomaly detection systems for IVN, in 2011 (Müter and Asaj, 2011).

Although, there are many promising development orientation in the field of automotive security, there are still many alarming questions related to the security vulnerabilities of nowadays transportation systems. To bridge the gap between the acceptable and the existing level of automotive security, it seems to be inevitable to investigate the interdisciplinary field of safety and security co-engineering in an integrated way.

4 Standardization

4.1 Safety

The basics of transport sector's functional safety field were laid down by CENELEC standards (BS EN 50126-1:1999 (British Standards Institution, 1999); CENELEC-EN 50128:2011 (European Committee for Electrotechnical Standardization, 2011); NEN-EN 50129:2016 (Royal Netherlands Standardization Institute, 2016)), which discuss the issues of railway transportation (CENELEC) focusing on Reliability, Availability, Maintainability, and Safety (RAMS). To ensure safety and to treat hazardous events, CENELEC identifies safety methods, which are applicable for system components. In accordance with this, CENELEC standards do not aim to handle critical issues, accidents related to autonomous transportation systems (Szalay et al., 2017). These accidents can be identified as SoS-accidents, since they can be primarily derived from the complex system of systems characteristic of the given event (Koschuch et al., 2019).

In case of the automotive sector, the specifications of International Organization for Standardization (2011) (ISO 26262-1:2011) are applied to guide design, test and validation processes in order to achieve the sector specific functional safety requirements. According to ISO 26262-1:2011, in case of safety, there is no risks related to the system, which could be derived from the faulty operation of an electronic component or which could not be justified by reasonable principles (ISO 26262-1:2011). However, it has to be emphasized, that this concept can still not properly handle possible system faults that can lead to SoS-accidents explained by the extreme complexity of the system. Furthermore, ISO 26262-1:2011 allocates relevant roles to human factor during the safety related processes of the system.

To response the challenges of autonomous transportation related problems, the automotive industry started to compile a novel standard discussing the Safety Of The Intended Functionalities (SOTIF). The main innovation of SOTIF (ISO/PAS 21448:2019) (International Organization for Standardization, 2019) is its purpose to step forward from the classical concept of component level functional safety into the direction of investigating system related requirements and contexts. This objective is mainly represented, on the one hand, by considering the influence of the surrounding factors on the system; and on the other hand, by investigating the effect of different use cases on the system. Due to this reason, SOTIF is much closer to addressing SoS characteristics of transportation system than other automotive standards. In addition, SOTIF contains a limited security interface as well, which can provide an effective connection to security domain in the future. However, it still focuses on automation level 1 and 2 (Schiaretti et al., 2017), which is still far away from autonomous systems. On the other hand, it is also obvious that novel approaches aiming to response to the SoS characteristics of transportation systems cannot replace the classical component level functional safety methods.

The System Safety standard of United States Department of Defense (2005) (MIL-STD-882E) aims to represent safety principles in the field of system engineering. Since this standard evaluates the safety of a system with a comprehensive approach, MIL-STD-882E can be applied for establishing the safety related standardization framework of autonomous transportation. On the other hand, neither security related recommendations nor regulation are discussed by MIL-STD-882E standard, which sets a limit on the adaptability of the standard to connected and autonomous transportation.

ARP4761 discusses system related issues of airplanes (Society of Automotive Engineers, 1996). The main methodological framework of this standard is rather based on a deductive logic. Problems are investigated from a general, system point of view. This concept fits to the requirements of system safety.

As it can be concluded, traditional safety related standardization framework does not reflect directly to security threats. However it is also reasonable to be considered that security related methodological connections are partly concern of some of these standards (e.g. SOTIF interface).

4.2 Security

General cybersecurity related aspects are summarized by the standard for "Information technology — Security techniques — Information security management systems — Overview and vocabulary" identified as ISO/IEC 27000:2018. This standard (International Organization for Standardization / International Electrotechnical Commission, 2018) contains the comprehensive summary related to Information Security Management Systems (ISMS). Furthermore, ISO/IEC 27000:2018 includes a generic dictionary for definitions applied in the security domain.

To develop a cybersecurity system and to ensure continuous development for the developed protection system the methods of ISO/IEC 27032:2012 standard, entitled as "Information technology — Security techniques — Guidelines for cybersecurity" identified as should be applied. This standard (International Organization for Standardization / International Electrotechnical Commission, 2012) supports the continuous development of the protection system, covering the following fields: information-, network-, internet-, and critical information infrastructure security.

Recommendations and regulations related to the automotive security specific aspects is going to be discussed by ISO/SAE DIS 21434 (International Organization for Standardization / Society of Automotive Engineers, 2020). The main purpose of the standard is to ensure a cybersecurity architecture and methodological background to support automotive domain in detecting and investigating vulnerabilities and in considering security related issues even during the design process of connected and highly automated vehicular systems. The application of the standard is especially recommended in case of certain safety relevant automotive functions.

Other technical standards in the automotive domain can also have strong connections to cybersecurity, especially when they focus on the field of information technology or communication. In this context, the IEEE 1609 standard family focusing on the "Wireless Access in Vehicular Environments" (WAVE) plays a key role in automotive security. The second section of the standard focuses on secure message formats and processing for communication devices applied in road transportation.

Due to the rapid development of automotive communication domain, other newly developed standards related to vehicular data and information exchange (e.g. ADASIS, SENSORIS) are expected to become important from a security point of view. These security relevant standards can either have strong security modules or should be closely connected and strongly reflect to the aforementioned automotive security standard.

5 Introducing the newly identified research orientations

Based on the introduced trends and evolution processes, it seems to be obvious that safety and security have to be an integral part of design process. Beyond this, it can also be concluded that safety and security can no longer be handled in a separated way.

Security can have direct influence on transport safety, since a successful malicious intervention from the cyberspace can have critical impact on safety related functions of the transport system. The exposure can even be more significant if the attack targets a more extended network domain or a larger group of system user.

On the other hand, safety related faults can also activate security vulnerabilities. For instance, in case of inappropriate function development or design processes, any physical damage caused by an accident can lead to the reduction of security functionalities. It is also needed to be emphasized here that, in some cases automotive safety and security are competing domains. With a simple example, if process resources are investigated (e.g. bandwidth or baud rate), the more resources available are, so the more informations accessible are related to the system operation processes, the safer the operation of the system can be. On the other hand, from a security point of view, limited accessibility can improve security and the restriction of available resources can increase protection, especially in case of a cyberattack.

Investigating this consideration, it can be a valid assumption that in case of a critical safety event, ignoring some of the cybersecurity protocols can be reasonable and necessary, which could cause serious vulnerability.

In light of the introduced synergies and restrictive interdependencies of safety and security, the integrated and interdisciplinary research of automotive safety and security has a significant importance. With regard to this research orientation, automotive safety and security related development of co-engineering methodology and validation framework are of key importance from the viewpoint of autonomous transportation. Accordingly, it is reasonable to emphasize that in case of testing and validating connected and autonomous transport systems, a scenario based, integrated evaluation of automotive safety and security would be closely fit to the concept of SOTIF and the SoS approach.

Beyond this, due to the particular importance of intra-vehicular communication, from the joint viewpoint of automotive safety and security, V2X communication will play a key role in future autonomous transportation system. In accordance with this, the communication and network security of "vehicle to everything" channels have to also be in the focus of automotive researches.

In accordance with the leading security strategies, in many cases, the detection of operation anomaly is more effective in preventing security incidents than the unreasonable improvement of protection system complexity. Thus the development of automotive anomaly detection systems, especially focusing on the complex SoS operation processes will be a highly important research orientation.

6 Conclusion

Since modern vehicles are connected and their transport processes are strongly supported by different automated functions, malicious external interventions can impair safety integrity.

Therefore, it seems to be reasonable in the future to introduce safety and security co-engineering approaches in the automotive industry.

To sum up the evolution of safety related functions in road transportation, it can be concluded that safety related functions can be classified in three relevant groups.

First system group contains the infrastructure related solutions especially considering traffic control and traffic management systems.

Beside this, vehicle related systems constitute another separated research field.

Furthermore, as it has been learnt from the review of system evolution processes, in case of the most up-to-date systems, communication based safety solutions started to play an outstandingly important role in the transportation sector.

Although, there are many promising development orientation in the field of automotive security, there are still many alarming questions related to the security vulnerabilities of nowadays transportation systems. To bridge the gap between the acceptable and the existing level of automotive security, it seems to be inevitable to investigate the interdisciplinary field of safety and security co-engineering in an integrated way.

Based on the introduced trends and evolution of standards, it seems to be obvious that safety and security have to be an integral part of design process. Beyond this, it can also be concluded that safety and security can no longer be handled in a separated way. With regard to the performed evaluation, three main promising research orientations have been identified.

In light of the introduced synergies and restrictive interdependencies of safety and security, the integrated and interdisciplinary research of automotive safety and security has a significant importance. With regard to this research orientation, automotive safety and security related development of co-engineering methodology and validation framework are of key importance from the viewpoint of autonomous transportation. Accordingly, it is reasonable to emphasize that in case of testing and validating connected and autonomous transport systems, a scenario based, integrated evaluation of automotive safety and security would be closely fit to the concept of SOTIF and the SoS approach.

Beyond this, due to the particular importance of intra-vehicular communication, from the joint viewpoint of automotive safety and security, V2X communication will play a key role in future autonomous transportation system. In accordance with this, the communication and network security of "vehicle to everything" channels have to also be in the focus of automotive researches.

In accordance with the leading security strategies, in many cases, the detection of operation anomaly is more effective in preventing security incidents than the unreasonable improvement of protection system complexity. Thus the development of automotive anomaly detection systems, especially focusing on the complex SoS operation processes will be a highly important research orientation.

Acknowledgement

The research reported in this paper was supported by the Higher Education Excellence Program in the frame of Artificial Intelligence research area of Budapest University of Technology and Economics (BME FIKP-MI/FM).

References

Abeysiriwardhana, W. A. S. P., Abeykoon, A. M. H. S. (2014) "Simulation of brake by wire system with dynamic force control", In: 7th International Conference on Information and Automation for Sustainability, Colombo, Sri Lanka, pp. 1–6. https://doi.org/10.1109/ICIAFS.2014.7069563

Amditis, A., Bimpas, M., Thomaidis, G., Tsogas, M., Netto, M., Mammar, S., Beutner, A., Möhler, N., Wirthgen, T., Zipser, S., Etemad, A., Da Lio, M., Cicilloni, R. (2010) "A Situation-Adaptive Lane-Keeping Support System: Overview of the SAFELANE Approach", IEEE Transactions on Intelligent Transportation Systems, 11(3), pp. 617–629. https://doi.org/10.1109/TITS.2010.2051667

Black, H. D. (1990) "Early development of transit, the navy navigation satellite system", Journal of Guidance, Control, and Dynamics, 13(4), pp. 577–585. https://doi.org/10.2514/3.25373

British Standards Institution (1999) "BS EN 50126-1:1999 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), Basic requirements and generic process", European Committee for Electrotechnical Standardization (CENELEC), Brussels, Belgium.

European Committee for Electrotechnical Standardization (2011) "CENELEC-EN 50128:2011 Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems", European Committee for Electrotechnical Standardization (CENELEC), Brussels, Belgium.

International Organization for Standardization (2011) "ISO 26262-1:2011 Road vehicles - Functional safety – Part 1: Vocabulary", International Organisation for Standardisation (ISO), Geneva, Switzerland.

International Organization for Standardization / International Electrotechnical Commission (2012) "ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity", International Organization for Standardization / International Electrotechnical Commission, Geneva, Switzerland. [online] Available at: https://www.iso.org/standard/44375.html [Accessed: 27 February 2020]

International Organization for Standardization / International Electrotechnical Commission (2018) "ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary", International Organization for Standardization / International Electrotechnical Commission, Geneva, Switzerland. [online] Available at: https://www.iso.org/standard/73906.html [Accessed: 27 February 2020]

International Organization for Standardization (2019) "ISO/PAS 21448:2019 Road vehicles - Safety of the intended functionality (SOTIF)", International Organisation for Standardisation (ISO), Geneva, Switzerland.

International Organization for Standardization / Society of Automotive Engineers (2020) "ISO/SAE DIS 21434 Road vehicles — Cybersecurity engineering", ISO/SAE International, Geneva, Switzerland.

Kandimala, N. R., Sojka, M. (2012) "Safety and security features in AUTOSAR", [pdf] Czech Technical University in Prague, Prague, Czech Republic, Available at: https://rtime.felk.cvut.cz/publications/public/autosar-safety-security.pdf [Accessed: 27 February 2020]

Koschuch, M., Sebron, W., Szalay, Z., Török, Á., Tschiürtz, H., Wahl, I. (2019) "Safety & Security in the Context of Autonomous Driving", In: 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE), Graz, Austria, pp. 1–7. https://doi.org/10.1109/ICCVE45908.2019.8965092

Liebemann, E. K., Meder, K., Schuh, J., Nenninger, G. (2004) "Safety and Performance Enhancement: The Bosch Electronic Stability Control (ESP)", SAE Technical Paper No. 2004-21-0060, Washington, DC, USA: SAE Ineternational.

Matheus, K., Königseder, T. (2017) "Automotive ethernet", Cambridge University Press, Cambridge, UK.

McShane, C. (1999) "The Origins and Globalization of Traffic Control Signals", Journal of Urban History, 25(3), pp. 379–404. https://doi.org/10.1177/009614429902500304

Müter, M., Asaj, N. (2011) "Entropy-based anomaly detection for in-vehicle networks", In: 2011 IEEE Intelligent Vehicles Symposium (IV), Baden-Baden, Germany, pp. 1110–1115. https://doi.org/10.1109/IVS.2011.5940552

Nadezda, Y., Foresti, G. L., Micheloni, C. (2017) "An ADAS Design based on IoT V2X Communications to Improve Safety - Case Study and IoT Architecture Reference Model", In: Proceedings of the 3rd International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS), Porto, Portugal, pp. 352–358. https://doi.org/10.5220/0006375303520358

Navet, N., Simonot-Lion, F. (2013) "In-vehicle communication networks-a historical perspective and review", In: Zurawski, R. (ed.) Industrial Communication Handbook, CRC Press Taylor&Francis, Boca Raton, FL, USA, HAL ID: hal-00876524. [online] Available at: https://hal.inria.fr/hal-00876524 [Accessed: 27 Febrary 2020]

Nilsson, D. K., Phung, P. H., Larson, U. E. (2008) "Vehicle ECU classification based on safety-security characteristics", In: IET Road Transport Information and Control - RTIC 2008 and ITS United Kingdom Members' Conference, Manchester, UK, pp. 1–7. https://doi.org/10.1049/ic.2008.0810

Oorni, R., Goulart, A. (2017) "In-Vehicle Emergency Call Services: eCall and Beyond", IEEE Communications Magazine, 55(1), pp. 159–165. https://doi.org/10.1109/MCOM.2017.1600289CM

Poletan Jugović, T., Čišić, D., Gumzej, R. (2019) "Supply Chain Service Quality Improvement by E-marketplace Automation", Promet - Traffic&Transportation, 31(2), pp. 185–194. https://doi.org/10.7307/ptt.v31i2.3042

Renner, M., Münzenberger, N., von Hammerstein, J., Lins, S., Sunyaev, A. (2020) "Challenges of Vehicle-to-Everything Communication. Interviews among Industry Experts", In: 15th International Business Informatics Congress (Wirtschaftsinformatik), Potsdam, Germany. https://doi.org/10.30844/wi_2020_r12-renner

Rivard, J. G. (1980) "Status of automotive electronics in the USA", In: 30th IEEE Vehicular Technology Conference, Dearborn, MI, USA, pp. 21–31. https://doi.org/10.1109/VTC.1980.1622788

Royal Netherlands Standardization Institute (2016) "NEN-EN 50129:2016 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling", European Committee for Electrotechnical Standardization (CENELEC), Brussels, Belgium.

Roads&Bridges (2011) "Amped-Up Traffic Signs Imminent for NJ Expressways", Roads&Briges, [online] 01 November 2011. Available at: https://www.roadsbridges.com/amped-traffic-signs-imminent-nj-expressways [Accessed: 26 February 2020]

Sari, Z., Brookes, D., Avery, M. (2017) "AEB Performance in the UK; A Decade of Development", In: 25th International Technical Conference on the Enhanced Safety of Vehicles (ESV) National Highway Traffic Safety Administration, Detroit, MI, USA, Article Number: 17-0290.

Schiaretti, M., Chen, L., Negenborn, R. R. (2017) "Survey on Autonomous Surface Vessels: Part I - A New Detailed Definition of Autonomy Levels", In: International Conference on Computational Logistics (ICCL 2017), Southampton, UK, pp. 219–233. https://doi.org/10.1007/978-3-319-68496-3_15

Schinkel, M., Hunt, K. (2002) "Anti-lock braking control using a sliding mode like approach", In: Proceedings of the 2002 American Control Conference (IEEE Cat. No.CH37301), Anchorage, AK, USA, pp. 2386–2391. https://doi.org/10.1109/ACC.2002.1023999

Society of Automotive Engineers (1996) "ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment", SAE International, Warrendale, PA, USA.

Szalay, Z., Nyerges, Á., Hamar, Z., Hesz, M. (2017) "Technical Specification Methodology for an Automotive Proving Ground Dedicated to Connected and Automated Vehicles", Periodica Polytechnica Transportation Engineering, 45(3), pp. 168–174. https://doi.org/10.3311/PPtr.10708

Tahat, A., Said, A., Jaouni, F., Qadamani, W. (2012) "Android-based universal vehicle diagnostic and tracking system", In: 2012 IEEE 16th International Symposium on Consumer Electronics, Harrisburg, PA, USA, pp. 137–143. https://doi.org/10.1109/ISCE.2012.6305105

Ullrich, G. (2015) "The History of Automated Guided Vehicle Systems", In: Automated Guided Vehicle Systems, Springer, Berlin, Heidelberg, Germany, pp. 1–14. https://doi.org/10.1007/978-3-662-44814-4_1

United States Department of Defense (2005) "MIL-STD-882E Department of Defense Standard Practice: System Safety", Department of Defense, Arlington, VA, USA.

Verendel, V., Nilsson, D. K., Larson, U. E., Jonsson, E. (2008) "An Approach to using Honeypots in In-Vehicle Networks", In: 2008 IEEE 68th Vehicular Technology Conference, Calgary, BC, Canada, pp. 1–5. https://doi.org/10.1109/VETECF.2008.260

Vestri, C., Bougnoux, S., Bendahan, R., Fintzel, K., Wybo, S., Abad, F., Kakinami, T. (2005) "Evaluation of a vision-based parking assistance system", In: Proceedings of the ITSC'05 8th International IEEE Conference on Intelligent Transportation Systems, Vienna, Austria, pp. 131–135. https://doi.org/10.1109/ITSC.2005.1520022

Xiao, L., Gao, F. (2010) "A comprehensive review of the development of adaptive cruise control systems", Vehicle System Dynamics: International Journal of Vehicle Mechanics and Mobility, 48(10), pp. 1167–1192. https://doi.org/10.1080/00423110903365910

Zöldy, M. (2019) "Legal Barriers of Utilization of Autonomous Vehicles as Part of Green Mobility", In: Prceedings of the 4th International Congress of Automotive and Transport Engineering (AMMA 2018), Cluj-Napoca, Romania, pp. 243–248. https://doi.org/10.1007/978-3-319-94409-8_29