KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 12, No. 2 (2022), p. 28 – 39

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)

Connectivity as a Tool for Safety in Automotive Transport

Konektivita ako nástroj pre bezpečnosť v automobilovej doprave

Jozef KOČÍK[1]

[1]*The University of Security Management in Kosice*

The manuscript was received on 09. 11. 2022 and was accepted after revision for publication on 01. 12. 2022

Abstract:

The topic of this paper focuses on the state of connectivity in today's cars, their limitations and further explores the possibilities of using connected cars with respect to safety. The first part focuses on defining the aspects related to connectivity, their subcontractors, the wide range of companies involved in development, their development genesis. These companies have been competing for a place in the market for the last few years with the most progressive hardware or software products. Cybersecurity is more than a hot topic of today, as European legislation has already enacted a regulation that obliges automotive manufacturers to have fully cyber secured new cars from 2024. In real life, we are faced with varying degrees of connectivity as our fleets age. The highest degree of connectivity then is the fully autonomous car of the future which development leader companies are now trying to develop. These are companies like VW, Audi, Tesla, Mercedes, BMW etc. and their suppliers. The last section explores the opportunities and development of new hardware, software, functions and services wit focus on the security.

Keywords: *connected car, connectivity, cyber security, autonomy car, technologies*

Abstrakt:

Téma tohto článku sa zameriava na stav konektivity v súčasných automobiloch, ich obmedzenia a ďalej skúma možnosti používania prepojených automobilov s ohľadom na bezpečnosť. Prvá časť sa zameriava na vymedzenie aspektov súvisiacich s konektivitou, ich subdodávateľov, širokú škálu spoločností podieľajúcich sa na vývoji, genézu ich vývoja. Tieto spoločnosti už niekoľko rokov súťažia o miesto na trhu s najprogresívnejšími hardvérovými alebo softvérovými produktmi. Kybernetická bezpečnosť je viac ako horúcou témou súčasnosti, keďže európska legislatíva už prijala nariadenie, ktoré zaväzuje výrobcov automobilov mať od roku 2024 plne kyberneticky *zabezpečené nové vozidlá. V reálnom živote sa s pribúdajúcim vekom našich vozových parkov stretávame s rôznym stupňom konektivity. Najvyšším stupňom konektivity je potom plne autonómny automobil budúcnosti, ktorý sa teraz snažia vyvinúť lídri vývojových spoločností. Ide o spoločnosti ako VW, Audi, Tesla, Mercedes, BMW atď. a ich dodávateľov. Posledná časť skúma možnosti a vývoj nového hardvéru, softvéru, funkcií a služieb s dôrazom na bezpečnosť.*

Kľúčové slová: *propojené auto, prepojenosť, kybernetická bezpečnosť, autonomne auto, technologie*

Introduction

The expression 'connected car' is one of today's most intensely debated buzzwords. There is no doubt that connectivity will shape the future of the automotive industry, but how? What will it mean for manufacturers, customers and customer services? What impact will it have on safety? These are the questions we often hear from not only clients in the automotive industry but from also from telecoms, tech, insurance and other industries, all of whom are going to be impacted by the connected car. In this article I would like to address these issues and to provide some practical examples. There are a multitude of definitions that are used when referring to the connected car. Each reflects the latest innovation but all are steps towards the revolution that will be the (semi-) autonomous vehicle. Yes connectivity will be an integral part of a vehicle's value, and will indirectly determine its value and running costs, but connectivity will also be our primary tool for increasing vehicle and passenger safety, and beyond that, the way in which transport functions within society.
.

1. The emergence of the connected car

Text Driven by the huge demand for the new digital technologies associated with connected cars, an ever-expanding list of companies from outside the traditional automotive supply-chain are playing an ever-growing part in the development of automotive systems. Spurred-on by this 'new' competition, automotive and traditional suppliers are also investing heavily in the resources that connectivity demands. The required level of technological hardware and software innovation to deliver 'intelligent', connected and ultimately autonomous vehicles, is a quantum leap and much of it has its roots in other industries. In 2015, Daimler, Audi, and BMW jointly acquired Nokia's precision mapping division 'Here', partly to prevent it from falling into the hands of a potential future competitor such as Google or Apple, but also to leverage external resources. This 'in-sourcing' is likely to become increasingly important especially with software development and artificial intelligence. Whilst the new-car development cycle can be as long as seven years, the software iteration cycle is typically measured in months, making coordination between the two cycles very difficult; even more so for artificial intelligence features such as ADAS and HMI systems that enable vehicles to learn the driver's preferences and driving styles, and to eventually achieve autonomy. To address this co-ordination issue and suppliers have been actively building up their in-house software capabilities over the last decade. A good example of the 'new' competition is Nvidia who started out by producing graphics chips for the computer gaming industry. In 2017 it entered the automotive market with its Tegra X1 chip which is capable of processing camera, radar and laser imagery, plus enabling machine learning. Companies like Nvidia have years of experience which they can leverage to build a substantial presence in the automotive sector which and traditional suppliers can only dream of for their competing technology. [1]

Fig. 1 Public illustration of a connected car in the future.

For some the answer is through acquisition such as Continental acquiring ASC’s Hi-Res 3D Flash Lidar business and its laser-based distance measuring technology. For others it is investment partnerships such as Delphi’s 2018 strategic investment in Quanergy, with the goal of jointly developing a low-cost Lidar system. (It is worth mentioning at this point that Lidar is a core technology for mass-market autonomous vehicles.) Yet another approach is technology co-operation agreements as seen with the 2018 Valeo and Mobileye agreement for the development of front-facing camera systems and of sensor fusion. (Sensor fusion is a technology that analyses the data input from numerous sensors to provide a more comprehensive insight than from just a single sensor eg, using multiple cameras to simulate depth perception). To address the difficulties of co-ordinating development cycles, Audi (in partnership with Nvidia) decoupled software development from the hardware development of its modular infotainment system, resulting in a new system within just 12 months. On a parallel track a variety of major software houses including the likes of Apple, Google, and Baidu, are vying to capture a share of the automotive infotainment market for themselves. Most producers now offer in-vehicle, smart-device mirroring systems, such as Apple CarPlay and Android Auto, whilst Baidu is gaining market share in Asia. Integration with smartphones is becoming a key-feature in infotainment, and ultimately vehicles will contain a mix of embedded and smart-device technology to provide infotainment features. Producers are actively using more HMI technologies from non-automotive companies such as Nuance, Immersion (haptics), and MyScript (for decoding finger movement). Developing similar technology in-house is often just not feasible, given that the automotive sector is comparatively too small a market to justify the cost for the development of such technology. [1]

2. The connected car and cyber security

Technology companies are realising that the connected car could easily be a cybersecurity nightmare. Hackers have already broken into car systems and taken over control of vehicle functions such as navigation and even some safety systems. Future break-ins could even affect multiple vehicles at once resulting in disrupted traffic flow or a ’grounded’ car fleet. And then there is the ever increasing flow of personal data that could be compromised, plus potential ’backdoors’ into the IT systems of the vehicle’s producers, suppliers and service providers. As digital functions and services become more sophisticated, such as the Mercedes ‘go faster’ subscription, hackers are most likely to focus on stealing the code that enables these additional features. Free distribution of software ‘cracks’ would seriously undermine the entire business case for the connected car. Consumer awareness of the cyber security problem is building, and could eventually lead to mistrust of the connected car, whilst the increased regulatory scrutiny to combat the problem could increase the vehicle’s cost. [2]

Connected cars are vulnerable because they are complex machines that combine an array of different digital systems, any of which might be a weak link. And they are built through the combined effort of producers and a host of third parties (both traditional Tier One suppliers and new entrants). No connected digital system is 100% secure but the connected car must be as secure as it can be, and it is the responsibility of the producers to achieve this. Apart from solving the purely technical issues, vehicle cyber security requires the proper project environment in which the right security software can be developed, tested, and maintained. Automotive companies are complex beasts with many competing interests. The development of a new vehicle forces the entire supply chain to focus on the next start-of-production date. Once that date arrives then the focus shifts to the next one. Meanwhile the previous iteration will stay on the market and in use for many years to come. Typically any updates require an expensive product recall, presuming that there is indeed an update to implement. Most producers simply don’t currently have the necessary development capabilities; they are not software companies whose strength lies in rapid innovation and the constant upgrading of complex computer code. The current producers development process for security software involves binding it to the vehicle’s hardware. As a result, updating the software, as well as any related back-end systems, is a very cumbersome process that is too slow to react to new threats. And because each newly developed car requires its own unique combination of hardware and software, producers need to support each and every version. But if a vehicle’s software can be updated remotely via its connectivity functions, akin to an operating system upgrade for a smart phone, then the process could become viable. Many producers are working on this but only a few such as Tesla have achieved it. The problem is how to integrate cyber security, a cross-department requirement, into the corporate structure. Cyber security touches upon every traditional department from design and engineering through to sales and finance, plus of course the multitude of 3rd party suppliers whose own systems must be as equally secure. How to allocate the overall responsibility is not the work of a moment. [2]

And then come the support functions that cyber security requires such as risk management, progress monitoring and reporting, incident management and testing. Traditional software development leverages its ability to issue continual upgrades to release any given version ‘as is’, but automotive requires nth degree testing. Who will write and compile the test catalogues that define the testing processes? Without them it’s not possible to determine if the software is fit for purpose, meets all the necessary quality and security requirements, or to identify and resolve any defects. [2]

Fig. 2 Public illustration of a secured car.

Once testing is complete and cyber security software is installed into vehicles then begins the requirement to identify and react to new threats, code new software and then somehow install it. No easy task given the complexity of the code itself, the co-ordination required throughout the supply chain and long product life-cycles. The processes for this work and their rigorous enforcement must be the responsibility of the producers. Clearly, strong cyber security is a critical success factor for the connected car. Not just to keep the vehicle and all of its connected services safe from hackers, but to build the level of trust needed to retain car-buyers as customers. The complexity of the technology and the processes involved in creating the connected car is what makes the task of the cybersecurity software development so difficult. Vehicles now have many systems that send and receive data, all of which are vulnerable to attack, as are the back-end systems that process that data. With each advance in what is technologically possible comes consumer scepticism about its safety. Think back to the humble remote keyfob and then start multiplying. One possible solution may involve cloud computing. Advances in cybersecurity now allow for embedded protection in distributed remote computing. Instead of focusing on firewalls, companies can monitor and track behaviour instead, with suspicious activity identified and isolated in real time. As the connected car becomes more common-place, opportunities will emerge to take this step to the cloud but given the complexities of securing the connected car and the sheer number of software programs that make the car connected, this step must be a collaborative effort. [2]

3. Vehicle services

Although the smartphone is still the most common form of in-vehicle connectivity, manufacturers are working on embedding connectivity within in the car itself. This can be divided into three areas: the underlying communications infrastructure, and then the vehicle services and device services which are supported by this infrastructure. [3]

3.1. Communications infrastructure

The major supplier is Valeo, who in 2015 acquired Germany’s Peiker to gain access to Peiker’s onboard telematics and mobile connectivity technology. And amongst the new entrants are Cisco Systems and NXP Semiconductors who, in 2016 , jointly invested into Cohda Wireless, a specialist in wireless communications for automotive safety applications. [3]

3.2. Connected vehicle services

These are services that can aid in the safety and management of the vehicle itself, such as remote vehicle diagnostics, cybersecurity, over-the-air system updates, fleet management, and usage-based insurance. The range of companies already active in the market is remarkably wide, including leading names from analytics, insurance and mobile network operators. In 2015, BMW and Pivotal formed a partnership to provide the former with ‘big data’ and predictive-analytics capabilities. This allows BMW to have a better understanding of the driver experience and insights into vehicle performance such as the correlation of part failures with driving conditions. [3]

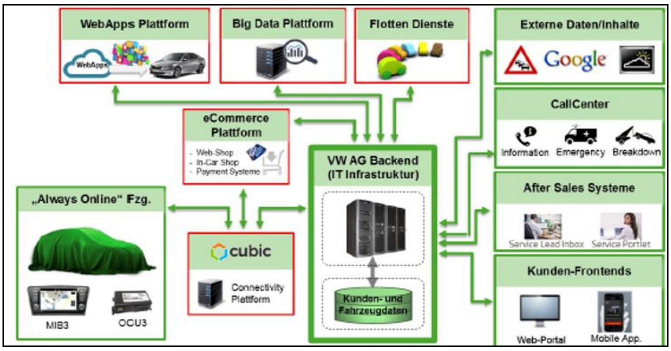

Fig. 3 Diagram of the connectivity system

3.3. Connected device services

These are services that are provided directly to drivers and passengers. They include smartphone-based services such as streaming, social media and integration with smart home devices. They also provide access to city services like traffic management, parking, and tolls. [3]

And although not a customer facing ‘service’ the inherent connectivity can be used by the State. Real-time speed data can be monitored for excessive speeds rather than deploying patrol cars, accidents can be forensically investigated with additional insight, and driver behaviour data can be used to modify accident blackspots. [3]

4. The limits of car autonomy

The connected car is an interim step on the way to the future of the truly autonomous vehicle, a future where we imagine vehicles picking up their ‘users’ on demand and transporting them to their destination in customised comfort along optimised routes before disappearing for their next assignment. Depending on your point of view, either this vision of the future won’t become reality for many decades, or it has already started. At the moment even the smartest cars are pretty dumb. They are programmed to do the same things for you that they do for everyone, regardless of personal preference. They lock the doors, they won’t let you move unless your seatbelt is fastened and they direct you along routes that make no sense to drivers with local knowledge. In many ways they’re marvels of engineering but they are generic marvels that behave in exactly the same way regardless of who is behind the wheel. But still-nascent technologies, notably AI, machine-learning and HMI, are promising to change all that. Even if the owner is a fleet operator, the car that comes to pick you up will recognize you, and reset its systems to meet your preferences. Your the seat will adjust to your preferred position, the infotainment system will log into your social media accounts or update you on breaking news, even the interior colours and lighting will be adapted to your choices. [4]

Fig. 4 Illustration of connectivity in practice

The goal is to build the intelligence and learning capacity into cars that will enable them to know who you are, what you expect and to predict what you will need. The ability to adapt and react will supersede the requirement to just do. This level of intelligence is already reaching maturity in industrial robotics where access to a wide range of sensors and network data provide a detailed overview of their workplace. This enables them to interact smoothly with humans, or call for assistance in advance of foreseeable problems. Of course road cars operate in much more complex and ever-changing situations and conditions so they need to be that much smarter. The input into to the machine learning system will also be that much more sophisticated. Autonomous cars are already equipped with sensors, cameras and laser systems that monitor the driving conditions and traffic situation, but now these systems will be present inside the car, observing and analysing the driver and taking action when appropriate. And your car will not just be learning from you but from every source that it can connect to, leading to a kind of swarm intelligence that will exponentially increase its understanding and learning potential, enabling it to combine its sensor data en mass and access cloud-based analysis to understand how to react. As you slow down to stop at a train crossing, another member of the swarm knows there is now time for a smoke break after tanking. The effort to increase vehicle 'intelligence' has been accelerating. In 2016, Toyota announced that it will invest more than $1 billion in AI over five years to improve car safety. Its business case: Better safety can be used as a major selling point. Whether AI and machine learning can become a unique selling point for Toyota, or for any other carmaker, will depend on just how far it can push the technology, and whether the advantages and features can justify the inevitable price increase. [4]

Nearly every car is now equipped with an LED screen through which you control the infotainment, navigation and climate control systems, and which provides the driver with car status data ranging from and fuel consumption and mileage range through to external temperature and tyre pressure. Yet for some reason the user interface for many of these control panels is woefully inadequate and often counterintuitive. Imagine what will happen when the amount of data that the connected car can access increases exponentially. How can this data be made available and be presented for manipulation. Intuitive HMI systems that incorporate voice, touch and sound as well as visual are a necessity. In today's market, there are already car companies that offer head-up displays on the windshield, but that should change in the future and they should start using side and rear windows as well. Passenger seats, including the driver's, could change tar and stiffness according to the moods of individual crew members, offering relaxation in the case of muscle stiffness, for example. [4]

The truly intelligent, fully connected car will require a massive amount of computing power and super-high-speed communications systems, both of which are already in development. The next step forward in connectivity will be fifth-generation telecom networks that can operate at rates 100 times faster than the current LTE technology. Vodaphone, Huawai, Nokia, Ericsson, Qualcomm, and Nvidia have together demonstrated such a network. And where these networks aren't available, short-distance Wi-Fi networks such as DSRC (dedicated short-range communications) will enable cars to maintain their connections. DSRC is already used to provide traffic-related information on highways. Current internal data networks which connect sensors, processors and controllers to HMI systems and Wi-Fi modules are not particularly fast, and are a long way from the speeds required for autonomous driving. There is a need to develop gigabit data transfer networks that will support the ultrafast chips required to process the incoming data, especially image processing from camera, radar and laser. Although some of the car's computing needs can be 'outsourced' to the cloud, responses must be instantaneous, 100% reliable and seamless when moving between network nodes. [4]

5. You can't stop development and innovation

Producers throughout the global automotive industry are working hard to make the vision of the connected car and autonomous vehicles a reality; experimenting, testing and building the technology that connects cars to the world around them, and the well-publicised development of prototypes that drive themselves. But there are still substantial hurdles to be overcome for this level of innovation to penetrate the mass-market, not least consumer perception of safety and privacy. But I believe that many of the individual components that together create the connected car are already here. [5,6,7]

Internal	**Strengths:** • cooperation of global car manufacturers • competition	**Weaknesses:** • conservative thinking • fear of using personal data
External	**Opportunities:** • increased security and new use of connectivity • development of new hardware, software, functions and Services • new start ups	**Threats:** • hacker attack • digital security • misuse of obtained data
	AUXILIARY	**HARMFUL**

Tab. No.1 SWOT analysis (own processing)

SWOT analysis helps us to describe the strengths, weaknesses, opportunities and threats for the connected car of the future. Subsequent innovation in this sector would look like the examples below

5.1. Bluetooth

Already widely used for in-car voice conversations via smartphone, Bluetooth can enable phone apps to utilise a car’s hardware for content display and interaction. In the near future, smartphone apps could be more fully integrated, allowing drivers to, for example, have the day’s scheduled events in their smartphone calendars displayed on the windshield. Cars will link user data such as calendar entries with other relevant information.

5.2. Navigation systems

The next step will be real-time traffic predictions with alternative routing in response to accidents etc. Further down the road, navigation systems will take the form of a head-up display projected onto the windscreen. This will be followed by augmented reality overlays of pertinent digital information, including alerting the driver to imminent hazards.

5.3. Telemetric insurance

Certain car brands already give car owners the option to have their driving style data stored and analysed for the purposes of personalised risk assessment, but greater connectivity can lead to far shorter feedback loops, and eventually to real-time 'pay-as-you drive' insurance. Knowing the speed, the route being driven, time of day, road conditions, and even who else is on the road can all be used to calculate a far more accurate risk assessment. Telemetric car insurance is very real.

5.4. Maintenance services

Current maintenance services already include alerts when mechanical problems arise but the connected car can take this a step further with the transmission of remedial fixes, damage prevention and workarounds until a service inspection can be scheduled. Dealerships and service centres will be involved as the connectivity of these services becomes increasingly sophisticated.

5.5. Driving assistance

System ADAS today make driving safer and more convenient with features such as „blind spot object“ and pedestrian detection, „lane assist“, active city safety, active cruise control radar, collision warning with full auto brake, and active park assistance. These options are today standard. ADAS's longer-term evolution is predicted to be autonomous driving – adding even more value to the driving assistance value proposition. By removing human error from the equation, fully autonomous driving promises nearly 100 percent safety and greater commuting efficiency, allowing the person in the driver's seat to do whatever a passenger may want to do, including working, reading, watching video, or sleeping. Ultimately, autonomous driving will allow for the entire redesign of the human-machine interface (HMI) and interior layout of the car. As an example of this, Mitsubishi presented a concept car at the Tokyo Motor Show already in the year 2013 that proved transform its interior layout from "cockpit" to "office/entertainment" mode. [5,6,7]

Another option is to detect the amount of alcohol in the blood based on the driver's breath, and if it is identified as positive, the inteligent car he'll be denied a ride in the car or its continuation.

5.6. Use of data by security forces

The police could use the data that the car transmits over the internet while driving to monitor traffic (speed, or accidents) without the need for radar measurements on the ground. In case of a driver speeding, a suitable operating system would be able to email the car owner a summons to explain himself.. In terms of security, there may even be a situation where driving a car yourself is illegal. Such an example (in case of connecting an inteligence car) can be imagined in a situation, where a driver who has had his driving licence suspended for his offences can be easily detected by security forces through connectivity and on-line data monitoring

Conclusion

In addition to emission-neutral powertrains and fuels, today's automotive industry is moving towards more and more connectivity. From today's simple internet-based systems, to highly sophisticated and advanced assistance systems, to fully autonomous cars. The speed of development and innovation in this sector is taking off with the development of digital, telecommunications and internet connectivity. It is up to us how we use and deal with these technological advances. It is our customers and users who determine which product or service we will or will not be interested in. One thing is certain, however, and that is that increasingly sophisticated and more sophisticated technologies, their software, hardware and communications are intended to take their use to a higher level, and we should not forget about the safety of ourselves and other people.

List of Abbreviations

ADAS: Advanced Driver Assistance Systems

BMW: BayerischeMotoren Werke

HMI: Human–machine Interface

LED: Light-Emitting Diode

SWOT: Strenghts, Weaknesses, Opportunities, Threats

References

Books:

[1] MEIPING, W., YIFENG, N., MANCANG, G., JIN, CH., *Proceedings of 2021 International Conference on Autonomous Unmanned Systems (ICAUS 2021)*. Singapore: Springer, 2021. p.443 ISBN 978-981-16-9491-2

[2] SHIHO, K., RAKESH, S. *Automotive cyber Security*. Singapore: Springer, 2020. p.216 ISBN 978-981-15-8055-0

Journals:

[3] KRIEGER, T., GERCHON, M., CORNET, A. Integration levels of conectivity. In: *Conncted car automotive value chain unbound*, 2014, vol. 54, no. 5, p. 26-50. avaible from:

https://group-wiki.wob.vw.vwg/wikis/display/autoportal/Autoportal+Home

[4] MOHS, J., HIRSCH, E., KOSTER, A., DIETMAR, A. Opportunities, risk, and turmoil on the road to autonomous vehicles. In: *Connected car report* [online journal], [cit 9-11-2022] Vol. 6, No. 5, avaible from:

https://link.springer.com/

Data, reports, thesis:

[5] BMW Connected Drive Web site, 2019-2021. [online]. avaible from:

https://www.bmw.com/en/index.html

[6] Mercedes-Benz Web site, 2021. [online]. avaible from:

https://www.mercedes-benz.com/en/zeitgeist/mixed-tape-music-now-on-spotify/

[7] Open Automotive Alliance, 2020. [online]. avaible from:

https://www.openautoalliance.net/#about

Autor:

[1]**Ing. Jozef Kočík –** external doctoral student, The Universtiy of Security Management in Kosice, Košťova 1, Košice, Slovakia, jozefkocik@seznam.cz