ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

University Of Piraeus

Postgraduate Program
«Techno-economic Management & Security of Digital Systems»

Master Thesis Subject:

«Connected Cars»

Supervisor: Dr. Kanellos Leonidas

MSc Candidate: Kalampoukis Ilias [Student ID #: MTE1547]

Piraeus 2017

INSCRIPTIONS

I would formally like to thank my supervisor, Dr. Leonidas Kanellos, for his contribution, mentoring and guidance throughout the dissertation's compilation. Each and every of his advices, led to methodically initiate, study, process and deliver a detailed report, able to bring up significant milestones in the selected topic, which he mutually agreed upon. His availability and quick response, made it effective and easy for me to track any information, resolve all inquiries and deeply understand the technical and legal aspects of telecommunications law successfully. For that, I am deeply grateful.

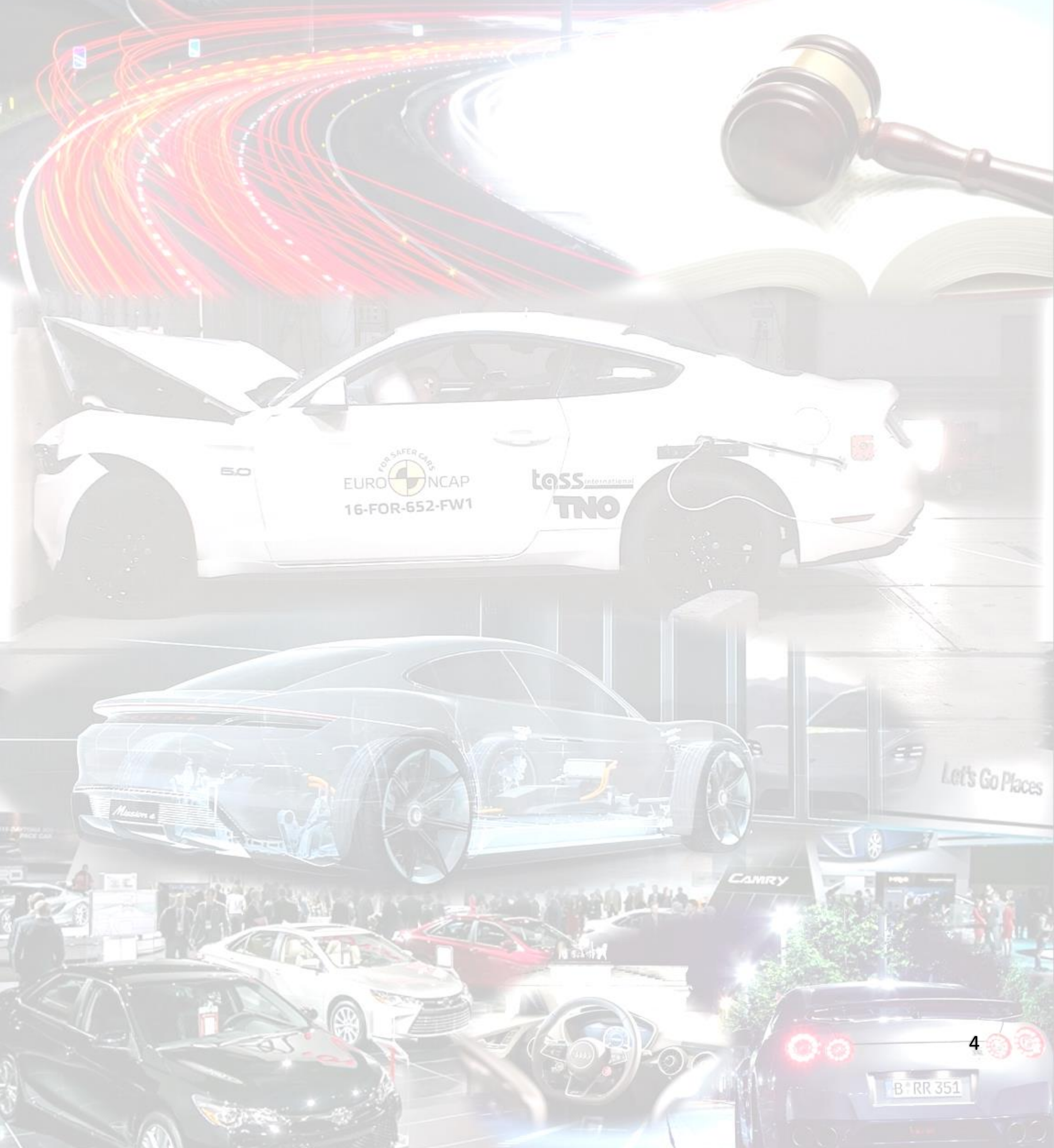
On a personal level, I would like to thank my family for their continuous support, as they were always there for me when I needed them the most. Finally, I would like to attribute my gratitude to my partner, Chara, for helping me whenever I was in need of assistance with my project, throughout the entire course's duration.

Εισαγωγή

Η παρούσα εργασία εκπονήθηκε στα πλαίσια περάτωσης του Π.Μ.Σ. «Τεχνοοικονομική Διοίκηση Ψηφιακών Συστημάτων» του Πανεπιστημίου Πειραιώς. Αφορά πλήρως επιστημονική και ερευνητική προσέγγιση των πτυχών του αντικειμένου με τίτλο «Διασυνδεδεμένα Οχήματα». Το θέμα αναπτύσσεται αρχικά με την περιγραφή των σύγχρονων αυτοκινήτων και την αλληλεπίδραση με τον ανθρώπινο παράγοντα. Εν συνεχεία εκτελείται μια ολοκληρωμένη ανάλυση του σύγχρονου εσωτερικού περιβάλλοντος του αυτοκινήτου, καθώς και του τρόπου που αντιλαμβάνονται οι χρήστες τις νέες τεχνολογίες στα σύγχρονα αυτοκίνητα. Προκύπτουν κάποια συμπεράσματα επάνω σε νέες υπηρεσίες που ήδη εφαρμόζονται ή βρίσκονται ακόμη σε πειραματικό στάδιο. Αναπτύσσεται μια ευρύτερη αναφορά στις επίσημες συνεργασίες κατασκευαστών αυτοκινήτων και τηλεπικοινωνιακών οργανισμών που έχουν προκύψει μέχρι σήμερα. Γίνεται μια σχετική προσέγγιση της σύμπτυξης των μοντέρνων οχημάτων με τις τηλεματικές και τηλεπικοινωνιακές υπηρεσίες και ορίζονται οι παράμετροι με τις οποίες αυτός ο συνδυασμός αρχίζει να εφαρμόζεται στην σύγχρονη αυτοκινητοβιομηχανία. Επιπρόσθετα, παραθέτονται υπηρεσίες προστιθέμενης αξίας που μπορούν να χρησιμοποιηθούν σε μοντέρνα μοντέλα προκειμένου να καλυφθούν επιπλέον ανάγκες των οδηγών και επιβατών, όπως η ορθή διαχείριση χρόνου, η μεγιστοποίηση ασφάλειας, πληροφόρησης και ψυχαγωγίας.

Γίνεται μια εκτενής αναφορά στα ζητήματα που προκύπτουν σχετικά με τις απαιτήσεις των διασυνδεδεμένων οχημάτων, τόσο σε τεχνικό όσο και σε οικονομικό επίπεδο (ετοιμότητα οδικού δικτύου, διείσδυση αγοράς, οικονομικοί παράγοντες, νομικοί περιορισμοί κτλ.). Περιγράφονται κάποια νομικά σενάρια που πρόσφατα προέκυψαν και σχετίζονται με τα επίπεδα πρόσβασης και κοινοποίησης πληροφοριών αυτοκινήτων (driver data-logs), καθώς και τα κύρια σημεία αξιοπιστίας τέτοιων συστημάτων ενάντια σε κακόβουλες επιθέσεις (hacking, απομακρυσμένος έλεγχος, κρυφή παρακολούθηση κλπ.). Εκτελείται αναφορά και στα αυτόνομα οχήματα, όπου εμφανίζονται ιδιαίτερες ανησυχίες σχετικά με την "συνύπαρξή" τους στους αυτοκινητοδρόμους, μαζί με τα αντίστοιχα συμβατικά καθώς και στις ιδιαίτερες περιπτώσεις ανάληψης ευθυνών ατυχημάτων. Τοποθετούνται νομικά ζητήματα τα οποία αφορούν στην ορθή και διασφαλισμένη εκπομπή πληροφοριών και δεδομένων μεταξύ οχημάτων, τηλεπικοινωνιακών συστημάτων και παρόχων υπηρεσιών. Ορίζονται επιπρόσθετα προβλήματα που προκύπτουν από την διαβάθμιση άρσης απορρήτου και τα νομικά εμπόδια που δυσχεραίνουν την εγκατάσταση τέτοιων συστημάτων καθώς και καταγράφονται οι απόψεις των χρηστών σχετικά με την κοινοποίηση ή μη προσωπικών δεδομένων (τοποθεσία, διαδρομή, ιστορικό πλοήγησης, καταγεγραμμένες ενέργειες οδηγού κλπ.) σε τρίτους, όταν οδηγούν.

Αριθμούνται τα εμπόδια ενσωμάτωσης των διασυνδεδεμένων οχημάτων (νομικών και τεχνικών) και σημειώνονται οι δυσκολίες εφαρμογής τους σε μαζικό επίπεδο. Καταλήγοντας, εξάγεται ένα γενικό συμπέρασμα ως προς την πορεία των διασυνδεδεμένων οχημάτων, τόσο σε ευρωπαϊκή όσο και σε παγκόσμια κλίματα, ωστόσο δεν παραλείπονται και κάποιες αναφορές σχετικά με την σωστή μελέτη, τον σχεδιασμό και την ενσωμάτωση αυτοκινητιστικής δια-συνδεσιμότητας στις σύγχρονες χώρες, συμπεριλαμβανομένων και των απαιτούμενων ενεργειών που θα οδηγήσουν στην επιτυχή υλοποίησή τους. Τόσο η μορφοποίηση όσο και το περιεχόμενο της εν λόγω διπλωματικής, ακολουθούν τους κανονισμούς του ΠΜΣ και σύμφωνα με την καθοδήγηση του επιβλέποντος διδάσκοντος. Η παρούσα διπλωματική εργασία αφορά προσωπική προσπάθεια μέσω διαρκούς έρευνας καθ 'όλου του διδακτικού εξαμήνου και αποσκοπεί στην ανάλυση ενός νέου θέματος, ως αρχικός οδηγός και προορίζεται για εκπαιδευτικούς σκοπούς.



Abstract

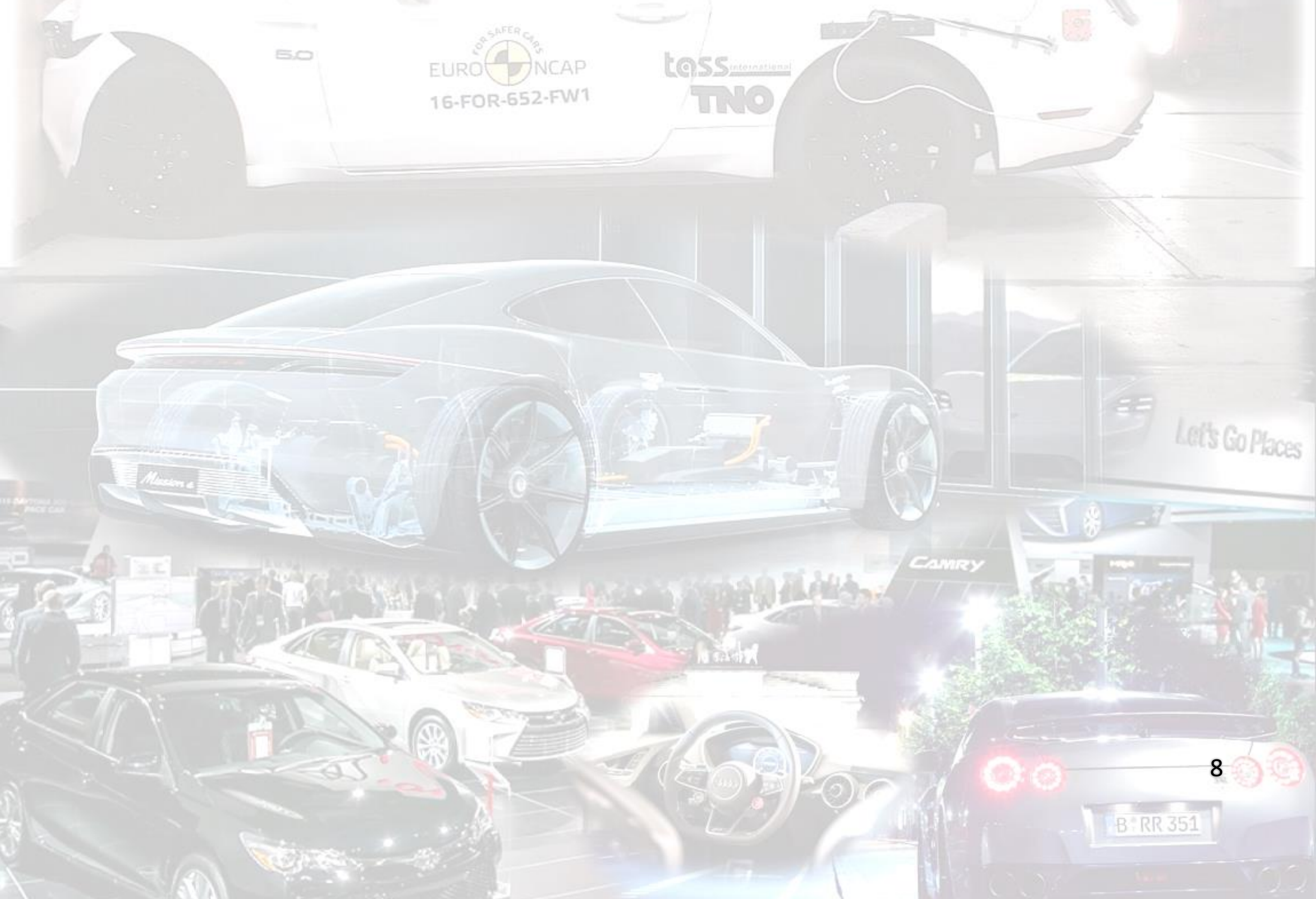
This dissertation was compiled and edited under the University of Piraeus's Post Graduate Program «Techno-economic Management of Digital Systems». It serves to emphasize the importance of vehicular connectivity as a modern aspect of the IoT world. Through detailed description of the automotive industry and its later tech implementations, an extended reference of automotive technology equipment is issued, including ambient factors, modern safety and information mechanisms and more. Initially, a vehicle – user experience analysis lists all the factors through which the infotainment systems are adjusted to the human behavior, mostly for driving assistance purposes. Up next, official surveys over dedicated analysis, reveal numerous topics, depicting the way governments (authorities) face this new connectivity platform, as new telecom and telematics services are steadily embedded into flagship models, during the last few years. In advance, a few significant value-added services are also listed, providing a clear view of how this connectivity shall enhance the lifestyle, positively and effectively.

Furthermore, the research includes a detailed report, identifying issues regarding connected and autonomous vehicle platform requirements on every single level (technical substance, economic impact, marketing penetration rate, legal barriers etc.). Some of the boldest technical and legal scenarios are applied, offering a certain aspect of today's accuracy and legality of connected systems, services and applications on modern cars. Through these examples, access issues and data privacy matters are stated (including technology failures, possible hacking cases, remote control attacks, private data access and illegal monitoring), giving the actual "image", hidden behind the current IoT modernization. Conclusions over legal guidelines are also developed, concerning security and privacy, along with data sharing of sensitive information such as user-vehicle location, access to driver logs, internet browsing history and 3rd parties' data access scalability.

Closing, various key points are recorded, in both national and international levels, recording main legal entities and data privacy protection vulnerabilities, as well as legal positioning of telecom vendors, 3rd party application developers and car makers in a balanced eco-system. Finally, without skipping suggestions over a safe and guaranteed deployment of connectivity platforms on a massive level, actions that will lead to a universal management system with legal and functional parameters are stated. The final conclusion over the connected vehicle era, leads to crucial approaches for the near future deployments that will prevail around the globe.

Keywords: CV platform, Vehicle-to-Vehicle, Vehicle-to-Infrastructure, Ambient, Infotainment, Telecommunications, Motorway, Application, Transmission, Modules, Autonomous vehicles, Over-The-Air, Framework, Automotive Market, Privacy, Security, Integration, Encryption, Standards, Defect, Regulations

Contents



Introduction

Technology and modern inventions are far beyond, the greatest factors that have until today, led to continuously drive the human lifestyle into persistent perfection. In year 2017, all aspects of modern life, have vastly been implemented into digital technology frameworks, providing easier procedures for the majority of the world's population. From the early show up of the television, till the very premature yet amazing virtual reality headsets, the human evolution tends to discover more and more brilliant new ways of fulfilling all needs for food consumption, education, entertainment, environmental consciousness, communication and transportation among developing and developed nations, worldwide.

In the 21ST century, many new techniques upgraded the way things in the daily life consist of. Tons of paperwork are now transformed into feather-weight bits & bytes, our old CRT televisions went on a diet and people who once used to write down notes with their blunt pencils, are now adapted to swiping their personal piece of glass instead (mobile phones w/touch screens).

The rise of the information age (and the use of Information - Communication Technology in particular) has brought about an increased emphasis on the collection, handling and distribution of all data flows that occur during any requested info exchange. Statistically speaking, our social life consists of no less than 73%, of personal data and automated procedures.

Those procedures include tax payments, internet-banking orders, logistics registrations, connection establishments, cross-function of state and private databases, self-health diagnosis gadgets and even successful faceless hotel or restaurant reservations. The amount of data being produced is dense, meaning it is always supported by adequate processing power and with the proper data analysis mechanisms. The last ones are the key to extracting all the useful hidden (dark) info, from initially categorizing the collected samples according to their common norms.

Up to this day, the great battles among the ICT industry (with all the blessings of the constant R&D findings), have proven the digital convergence will focus deeper and deeper on anything that has to do with remote communication plus information exchange, collection and analysis. No wonder, why all cell phone manufacturers have reached insane data speeds on their flagship devices in just a dozen of years. The centralized model demands everything go via our handheld devices, including correspondence to our ID details, to any credit data and even vital indications of the human body.

So far, so good…But what comes up as the next step of technological innovation, according to current trends and needs? Interconnected cars, that is correct. It's the new hot topic, the arrival of a new era and a completely different perspective of the - not so distant - future. Without a doubt, the last 5 years, have been especially fruitful, in terms of technologic excellence. Some of the market's leading automotive corporations, such as the VAG Group, the Mercedes-Benz Automotive Alliance, the Volvo Cars Corporation and the Lexus-Toyota car scheme, have enhanced their fame and reliability, by utterly developing their flagship products year after year. By providing new ways of mechanical efficiency on their models, upgrading new Infotainment Systems, developing safer protection standards for both passengers & pedestrians and with advanced & updated electronic integrations, these manufacturers have placed their own terms in the "game" of the modern automotive industry.

That have been said, telecom operators also seem to take place in that "game", where along with automotive manufacturers, a fresh convergence transforms into one plain new direction which will result in the massive effect of IoT around the globe. The action points between those two factors will be held by editing and standardizing existing and new regulations and legal frameworks that need to be precise at every single aspect, in order to maintain the current transportation environment, without violating user rights, or putting them and their constitutional substance into risk, at all costs. Those regulations is what car makers seek, for which the whole production lines will demand to be re-designed and adjusted so that they can face the new market needs, considering the size of it.

Conflicts and collisions are not missing from this new team-up strategy, especially on behalf of car makers, who require preserving the overall vehicle experience, the way people receive it, through the last fifty years. This dissertation will identify and categorize what the technology implementation offers, what advantages and disadvantages emerge, what the users shall experience or will receive as an outcome of the connected vehicles in their lives and what rules and restrictions should be applied, from both players.

Recent studies show that no step could be taken without the governmental cooperation, for as far as it is concerned, the motorways and road networks aren't yet ready or tech-compatible for this new perceptive transportation model. The outcome of all the above topics, will lead to some critical approaches on what this new connected world will lead to, including all influential parameters and legal factors.

Chapter 1st

The Era of Connected Vehicles

1.1. The Vision of Connected Vehicles

Vehicles have through time gained different substances, starting from them as early inventions many years ago, up to this day's modern multi-purpose tools. From the very first steam engines till the modern hybrid synergy mechanical sets, vehicles took part in becoming a vital demand on everyone's daily lifetime.

The need to eliminate distances and reaching points at ease and comfort, as well as the assistance in carrying stuff and constructing buildings and sites, placed the urban mobility on the top level of the human needs pyramid, right after nutrition and social interaction. Up to this day, many corporations co-exist with one and only purpose, to offer people the way to fulfill those needs, by providing the interested target groups with their main products, automotive vehicles. Cars, buses, trucks and motorbikes are the most frequently used automotive compounds all around the world.

Each and every vehicle category, serves different purposes and people evaluate their needs before buying the ideal vehicle, according to their priorities and needs. Constructional and civil engineering corporations have more professional equipment in their possession, while other targeted groups use civilian vehicles to serve themselves. The huge motorways around the globe support a well-managed traffic regulation system, that defines when and where each automotive category is allowed to execute routes under certain law obligations, in order to protect the civil environment as well as the drivers' safety, at all moments.

It was not long ago that car manufacturers had in mind, a futuristic approach of the public transportation, which would centralize into their automotive products. The massive steps of technology and innovation, ordered that anything people use in their daily routines, be upgraded along with the general evolution of modern life. This approach was initially held as a very promising scenario, where vehicles would have their own artificial intelligence and could easily scan for vital signs and emotions, as well as predictive analysis that would accurately avoid unwanted collisions.

More of this scenario was supposed to consider high-end civil vehicles to interact between each other, in the same or in similar ecosystems where all surrounding values are active identifiable entities that complete the standalone vehicle equity. Eventually, vehicle innovators dreamt of a universally compatible platform that would be accessed and applied equally across the world.

Consequently through years, all vehicles adopted suspensions, later hydraulic breaks, electric steering assist modules and even digital equipment. Some automotive producers still hold the tradition to innovate, by offering solutions to many market groups, by properly designing vehicles according to certain needs. Station wagon cars are focused on families and people who pack many things up. Convertible vehicles offer a personal status for their owners as they are rather rare to see on the streets (and usually two seated). High BHP cars serve excitement and velocity potential performance while city cars (Smart, VW Fox etc.), offer urban flexibility downtown. Above all, the automotive vision stated no discrimination between vehicle utilization or production differentiations.

1.2. How the IoT affected the Automotive Industry

All of these add-ons were of crucial importance in car evolution, as they both offered upgraded user experience and improved safety mechanisms. Yet for more than 50 years, the main problem still hasn't been totally resolved. Vehicle accidents have cost millions of lives every decade, despite any manufacturers' implementations or government automotive regulations.

It was not long ago that car makers started using safety airbags on the cabin's interior, for collision or accident protection. They came right after the three-point seatbelts which were patented and officially standardized by Volvo. As vehicles evolved in horsepower and appearance, each state and government dropped new regulations and restrictions, based on vehicle structure, safety certifications and constant evaluation of a ton separate requirements, as globalization led to the widespread use of automotive transportation. As an urgent need to eliminate this factor, the Euro NCAP performance assessment was founded by the Transport Research Laboratory in Brussels and approved by many European Government Civil Transportation Departments and the EU. The role of this authority was to ensure all safety specifications were followed by car manufacturers, once having their models released in the market.

Close to this authority, the respective Environmental Departments, also established a committee that would evaluate very strict regulations based on CO_2 fuel emissions on combustion engine vehicles, demanding constant mechanical upgrades that would confront with technology enhancement and environmental protection, mainly purposed to reducing harmful pollution factors (overall fuel efficiency, longer engine life expectancy, emissions elimination, etc.).

All those groups eventually cooperated with state troopers and police departments, in order to ensure all regulations were applied by the law, for all civilians without exceptions. Although regulations were fully utilized as public safety factors, the modern trends overwhelmed the population's lifestyle, meaning everything that was not digitally transformed, would sooner or later come to extinction, as new trends appeared.

It was near 2000, when the whole world started getting into a new shape, with the early adoption of the World Wide Web (Internet access) as a great globalization factor. E-mails, instant messages, colored LCD panels, multi-CD technology, remote controlled car parts (mirrors & alarm systems) and navigation compatible equipment initiated the forthcoming convergence. Technology created new paths of covering certain needs, such as brighter LED lights, automated air-conditioning, electric car windows and MP3 radio systems.

Such enhanced equipment was initially included in luxury versions of best-seller vehicles, for a greater price than that of standard base models. Cars went on a whole new appreciation and technology turned them from simple transportation tools into infotainment systems that had to offer more than a multimedia station itself. As years went by, car manufacturers tended to evolve their production line models by trusting more and more the digital technologies that appeared, offering solutions to smart mobility, enhanced user experience and modern external kits that would fulfill all consumer preferences and tensions.

The digital implementation promised precise vehicle handling and diagnostics that would offer accurate control of the separate car components (steering wheel, engine alarms, heating indication, tire pressure, seatbelt sensors and many more). The conclusion of such an approach demanded that vehicles would be better controlled and monitored by digital mechanisms, reaching the Internet of Cars. Through serious experimental sessions, it was further evaluated that vehicles could be fully inspected via Over the Air (OTA) technologies, in real time.

The very first car connectivity simulation was that of few vehicular pairings with specific cellular smartphones, offering an authorization as to who was behind the steering wheel, by simultaneously providing actual location tracking and partial access to the supervising authorities. It was as simple as the cellular connections themselves but the idea was based upon the cellular service that was automatically forwarded via each vehicle's ECU, overriding the smartphone connection.

As mentioned above, technology showed up in various ways and uses, attracting this way, car manufacturers, as a path to extend vehicle value through automations and integrated services. Audiovisual equipment was one of the initial add-ons on cars, upgrading the end user experience with deep bass and crystal clear music support. Later, analogue TV compounds, led the way to transform the vehicles into primitive multimedia stations.

After 2007, the first touch screen LCD displays made their way through expensive cars as they could assist Bluetooth connectivity, micro-SD card readers and navigation maps. It was at this checkpoint, where car manufacturers stopped integrating any significant or alternative tech-upgrade on their vehicles, other than few safety mechanisms, such as ABS systems, lane assist sensors and passive seats for head-on collisions.

Today, while there are lots of car companies that prefer to stay away from touch displays with big screens present in the head unit of their cars, many provide a hybrid option of having a touch display that can also be controlled using knobs and buttons. So manufactures actually found out that any single tech gadget or application, shouldn't just exist somewhere in the drivers cabin or ECU, but instead should approach a user-friendly experience, while offering real assistance in both security and entertainment.

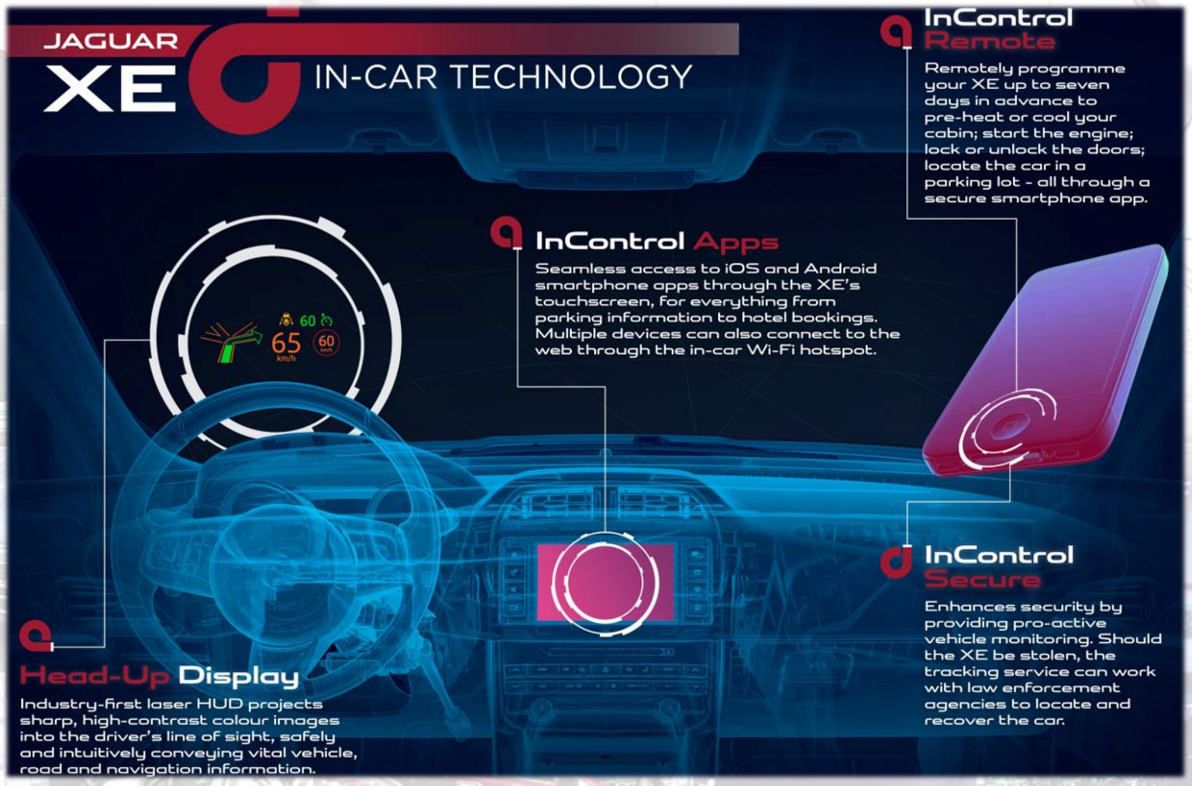


Image 1: *Jaguar's interior ambient, combining an OEM monitor console with buttons, wireless connectivity and intelligent dashboard, under a secure environment*
(trafficsage.org, 2016) [1]

The modern cars' main consoles have lately been selected as the ideal place for installing the central control panel for most of nowadays vehicles' functions. The head unit's interface on the other hand, proved to be of a much greater distraction, often causing accidents, as claimed several times in the past. Automotive researchers have been putting effort on developing the most suitable shared area HUD, while including the front passenger in the overall car management.

The purpose of such plans, was to create a central control station that would not only help the driver during a trip, but would also involve the front passenger even more in the decision making process. In terms of budget and economic values, this would demand an additional touch screen implementation on the front passenger's side that would unhopefully lead to an augmented manufacturing cost (as a standard / default vehicle equipment) [1]. The concept was very enlightening but the extra passenger display, would only prove to be useful if the front passenger was present in the vehicle (limited practical application).

Tesla Corporation had already taken into account the innovative face-lifting of shared vehicle management units, by modifying the main console, making it more visible and loading it with the proper user interface (colored resistive touch screens & software). Despite that, more and more applications emerged as Android, Windows & iOS platforms evolved through the smartphone era, for the last decade.

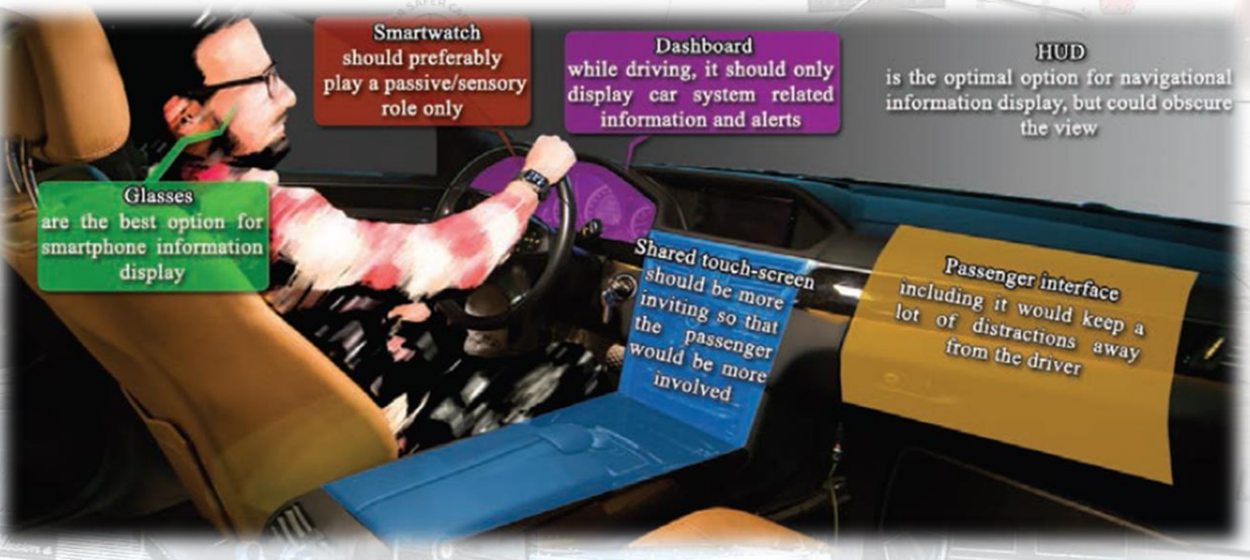


Image 2: *A demonstration of the ideal vehicular infotainment ambient based on the conclusions of the official car infotainment research* (Procedia C.S., 2016) [2]

Electronic control units were finally not functional exclusively for car diagnostics and service indicators, but started gaining digital intelligence, enriching those platforms, which could support lots kinds of applications, according to certain end-user preferences. 3D navigation, real time news feedback, Internet services, mobile phone HUD mirroring, Car Play console simulation and fuel management are only few of the nowadays countless applications a modern car can support.

After all, car manufacturers are on a full effort to equip vehicles with multiple compatible communication technologies such as Bluetooth, data transmitted via radio waves and Wi-Fi. The challenge here is to sustain enough processing power needed for these technologies, something not always available. More ECUs combined can support the multitasking abilities of the variant communication protocols and techniques, more effectively [1].

Although an ECU is a vital part of an integrated electrical system and the car's control center, it is a late technology trend, equipping more ECUs on motherboards, in order to manipulate and control the various parts of the vehicle that have a direct effect on the driving experience. ECUs have -in security terms- enabled features such as: Park Assist, Adaptive Cruise Control, Collision Prevention and many more driving mechanisms. The majority of these assistive tools have proven to minimize accidents and significantly upgrade the driving experience.

The vast majority of the world's population uses a car on a daily basis and the numbers of active driving units that co-exist in national and urban road networks are increasing with an aggressive pulse. The prevailing situation proves that all those assistive systems need to be integrated in the standard equipment of any commercial vehicle, as safety limits get thinner and more vulnerable to all surrounding values.

1.3. The First Interconnected Vehicles

General Motors was the very first automaker to bring the primitive connected car features into the automotive market with the OnStar platform in 1996. The specific platform was available in Cadillac DeVille, Seville and Eldorado models only.

OnStar was shaped by GM's cooperation with Motorola™ Automotive Laboratories. The primary purpose was safety features and emergency support for a vehicle, on any accident occasion. The sooner medical help arrived, the more likely the drivers and passengers would avoid fatal consequences.

A cellular telephone call would be routed to a call center where the agent sent help. That initial implementation only lasted a few months, as the network coverage on GPS and cellular coverage were not wide available in America, plus those services were only included in luxurious vehicles. In addition to that, the emergency system would only operate when at least one airbag was deployed. Other similar connected car platforms that were later released in the market are listed below [2]:

- ✓ By 2003, connected car services included vehicle health reports, turn-by-turn directions and removable network access devices.
- ✓ In 2007 Continental introduced data-only telematics.
- ✓ The first mass deployment of 4G LTE was released by General Motors.
- ✓ In the summer of 2015, Audi A3 was the first production line model to offer 4G LTE Wi-Fi hotspots access.
- ✓ The OnStar platform revived through the new 2016 Opel Corsa model as standard equipment, offering global car connectivity & geo-detection for collisions and accidents reporting.
- ✓ Telefonica agreed upon a partnership with the greatest electric car maker Tesla in major Western European markets.
- ✓ Orange also works with Tesla, in France, alongside other deals with Peugeot and Renault. Orange is also launching smartphone service Orange Drive, which offers users voice-activated radio controls and tips on efficient driving.
- ✓ Vodafone has signed up with Germany's BMW and, in August, bought Italian car services firm Cobra Automotive. Deutsche Telekom also made partners with BMW and joined China Mobile, the world's largest mobile provider, in a connected cars action.
- ✓ In China, Audi announced its cooperation with Tencent, on location sharing applications in vehicles.
- ✓ Peugeot and Citroen PSA teamed up with Alibaba, on a future smartphone application development that will remotely diagnose the vehicles' location and current fuel level.
- ✓ China Mobile and Deutsche Telekom signed a deal, in order to establish a CV platform in the Chinese market.
- ✓ American Airbiquity and Chinese Baidu connectivity vendors formed a strategic aligning that will soon release connected car Internet Services to the Chinese automotive market.

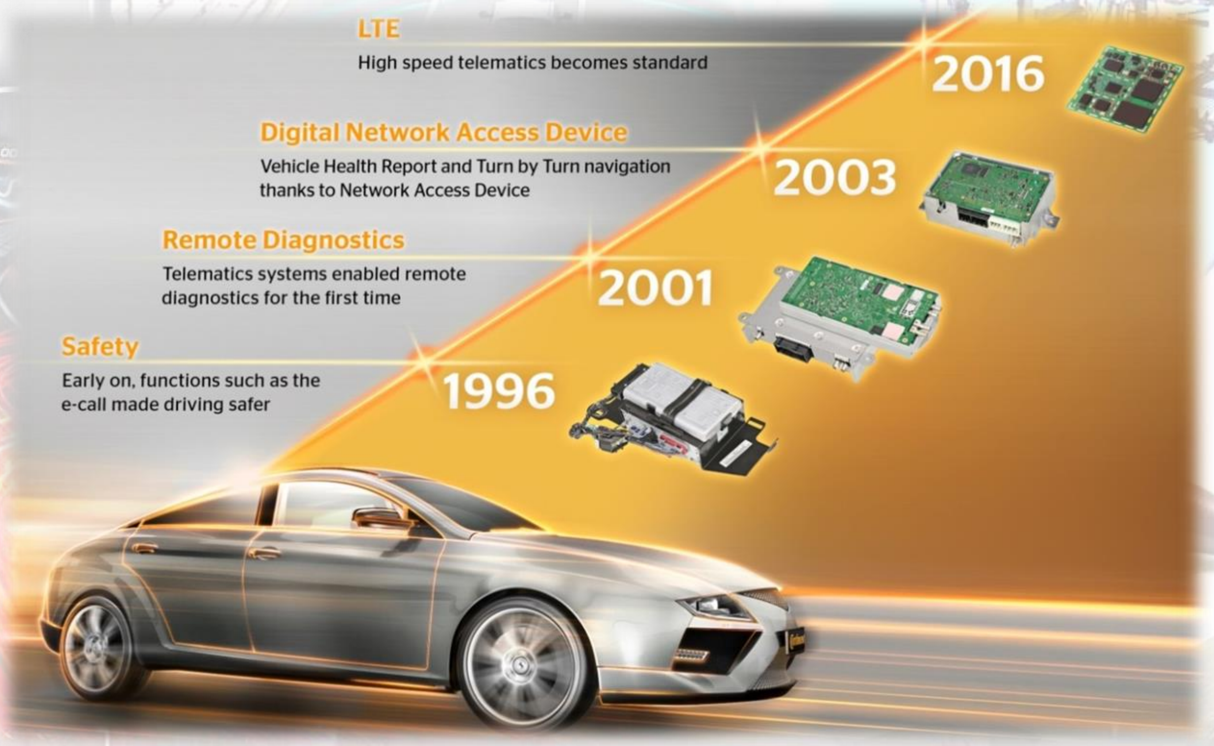


Image 3: *10 years of evolution in the connected cars technologies (1996-2016)*
(Continental, 2016)[3]

The modern world was predicted to be "connected", by standard rules that would be functional and compatible across different platforms.

Microsoft Office Suite was the very first to be 100% compatible across different computer operative systems, that were all able to understand that one common programming language, while offering a variant visualization in office documents.

Till this day, many of the leading global telecommunications vendors have developed unique connected vehicles or IoT divisions and forged partnerships to capitalize on the emerging profitable car market. Those alliance groups went into pre-release professional experimental testing of interconnected vehicles around America & Europe.

Standard protocols existed in almost all makes of business or personal smart tools, implying that the innovative tech-convergence became dense and was effective immediately supported by different tech-parties.

OEMs (major automakers)					
Acquisition Audi/Daimler/BMW: Here (2015) GM: Cruise Automation (2016) *Investment* Volvo: Peloton (2015) *Partnership* Audi & Nvidia (since 2005) Bosch & TomTom (2015) GM & Mobileye (2015) VW & Mobileye (2015) BMW & Intel & Mobileye (2016) Hyundai & Cisco (2016)	*Investment* Ford: Livio (2013) *Partnership* Audi & Nvidia (since 2005)		*Partnership* Daimler & Qualcomm (2015) Hyundai & Cisco (2016) Toyota & KDDI (2016)	*Partnership* Ford & State Farm (2012) BMW & Pivotal (2015) Ford & Microsoft Azure (2015) Volvo & Microsoft (2015) Nissan & Microsoft Azure (2016)	*Acquisition* Daimler: Mytaxi (2014) GM: Sidecar (2016) *Investment* BMW: RideCell (2014) BMW: Zendrive (2014) GM: Telogis (2014) BAIC: Didi Chuxing (2015) Ford: Pivotal (2016) GM: Lyft (2016) Toyota: Uber (2016) VW: Gett (2016) *Partnership* BMW & Baidu (2015) BMW & Microsoft Azure (2016) Seat & Samsung & SAP (2016) Toyota & Microsoft Azure (2016)
Traditional suppliers					
Acquisition Continental: Elektrobit (2015) Delphi: Ottomatika (2015) ZF: TRW (2015) Continental: ASC (2016) *Investment* Delphi: Quanergy (2015) Bosch: AdasWorks (2016) *Partnership* Valeo & Mobileve	*Acquisition* Harman: Aha (2010) Harman: S1nn (2014) Continental: Elektrobit (2015) Harman: Symphony Teleca (2015) *Partnership* Harman & Luxoft (2011) Harman & Microsoft (2016)	*Acquisition* Continental: Elektrobit (2015) *Partnership* Valeo & Safran (2013)	*Acquisition* Bosch: ProSyst (2015) Valeo: Pelker (2015)	*Acquisition* Harman: Redbend SW (2015) Harman: TowerSec (2016) *Partnership* Valeo & Capgemini (2015)	*Acquisition* Harman: Aditi (2015)
Acquisition Panasonic: Ficosa (2014) Google: FCA (2016) Nvidia: AdasWorks (2016) *New entrants* AdasWorks, Baselabs, Vector, Velodyne, Wind River	*New entrants:* Apple, Baidu, Google	*Investment* Intel: Omek (2013) *New entrants* Atmel, Fujitsu, Kyocera, LG, Toshiba	*Acquisition* Cisco/NXP: Cohda Wireless (2013) *New entrants* Cohda Wireless, Kymeta, Veniam	*Investment* Verizon: Hughes (2012) *Partnership* Airbiquity & Arynga (2016) *New entrants* Airbiquity, Allstate, Fleetmatics, Pivotal, Progressive, SiriusXM, Trimble, Verisk	*Partnership* Daimler Moovel & IBM (2014) Airbiquity & Arynga (2016) *New entrants* Airbiquity, Apple, Contigo, Dash, Google, iTrack, Lyft, MyCarTracks, Uber

Table 1: ***Automotive manufacturers and technology suppliers, as previewed by their partnership status*** *(PricewaterCoopers, 2016)* [4]

Luckily, some modern vehicles found themselves into this tech merging as well. Car manufacturers were more than positive into taking this convergence to a next level, by visualizing a world that would be more than just existent. The expanded vision was all about, creating an active transportation environment that would have the ability to self-adjust its structure partially or in total, according to specific values and based on their standard deviation.

Image 4: *Audi A3 Sport-sedan 4G, the first ever car with embedded 4G-LTE data connection chipset, was released in the US Market in 2015* (Car & Driver, 2015)[5]

Traffic lights needed to be smart and able to calculate the amount of surrounding vehicles, while instantly processing and exporting an urban traffic tension that would eventually serve more vehicles than standard programmed lights ever would.

The same pattern could also be applied on location-based applications that can find alternate routes to reaching final destinations at the same time with avoiding traffic jams and efficiently managing fuel consumption levels. Smart cities were initially conceived as a major idea, few years ago, when capital cities became overcrowded by vehicles, without providing any flexibility.

According to Audi A.G., cars must always be able to communicate with city traffic lights to find out when they will turn red, with soft display notifications implemented in each vehicle's dashboard. The next step of this transformation should unavoidably include cars that have the ability to communicate with each other to work out best patterns of lights through urban routes.

This technique is estimated to eliminate almost 60% of the physical traffic lights installed on motorways, leaving vehicles "define" the whole traffic management, even when the local urban electricity provision is interrupted.

Image 5: *Concept of the smart personalized "wind-shield" display currently under Audi testing, eliminating physical traffic lights, thanks to V2V communication* *(dailymall.co.uk, 2014)* [6]

The greater image behind this consideration was that cars and vehicles in general, would be ready to join mega metropolitan access or V2V local networks, according to their geographic location, while receiving a real-time feedback, for a safe and effective driving behavior.

In the same path, lies an analytical algorithm that processes intersections' vehicle flows, efficiently enough to ensure priority and security among transportation. Collected and categorized information produced by connected vehicles stats, such as the recorded position and speed of individual vehicles or the number of passengers, proved essential for utilization to adjust and enhance traffic operations at any small or dense intersections. It was generated on April 14, 2014 and only a certain percentage of cars are equipped with this technology.

The algorithm applies on two one-way-streets and processes different sequences of cars exiting intersections [3], resulting in minimum response times and effective traffic flows. Benefits of cross-junctions management (multiple cars consecutively discharging from a queue) and signal flexibility are also considered.

The intersection algorithm was tested to gain insights about the value (in terms of delay savings) of using connected/autonomous vehicle technology for intersections control, by manipulating the incoming and outgoing time fragments that can synchronize all approaching vehicles, by providing lower energy consumption, effective traffic management and collision avoidance mechanisms. Different simulations were conducted for equivalent total demand values and ratios, to comprehend the effects of changing the minimum green time at the signals and the penetration rate of connected cars.

By utilizing autonomous vehicle control systems, the signals could rapidly change the direction of priority without relying on the reaction of drivers. However, without this technology a minimum green time [3] was necessary. The results of the simulations showed that a minimum green time increases the delay only for the low and balanced demand scenarios and not for heavy traffic congestions.

Image 6: ***Tesla was the first automotive industry to "engage" with Telefonica, in an agreement to provide its autonomous vehicles with cellular car connectivity across European countries*** *(telematicnews.info, 2014)* [7]

Therefore, the importance of deploying cars with autonomous vehicle control can only be seen at intersections with this kind of demand patterns and could result in an estimated decrease in delay of up to 7% [3]. On the other hand, processing information from surrounding connected vehicles to synchronize the traffic signals and flows has proven to be significantly useful, as long as minimum response times are guaranteed (minimum delay fragments). For example, an above 30% ranged penetration rate, has given ambitious samples of a reduced average delay between vehicular transmissions.

Above that rate and for as long as the traffic congestion expands, the rate of reduction decreases accordingly and the marginal value of information from communication technologies, practically tends to zero. In total, it is concluded that such connected vehicle technologies are capable of managing heavy urban traffic phenomena, when applied at signalized intersections across motorways.

For similar algorithms to successfully apply in these scenarios, a deeper research is required, specifically on the following values:

- ✓ The selection of one of the three general approaches, naming them below:

  (i) fixed-time approach
  (ii) actuated approach and
  (iii) adaptive approach

- ✓ The collection, analysis and processing of historical traffic data

- ✓ The proper traffic signaling control

Chapter 2nd

The Connected Cars Technology

2.1. Advanced Tech Solutions

No surprise, the upgraded transportation solutions emerged in just a few years. A vast combination of different wired and wireless methods, created a uni-body, full of processing power and instant reflexes. Multiple ECU set-up motherboards turned vehicles into really powerful interconnected entities. Few years ago, some telemetry algorithms, offered a very promising scenario outcome, over which automobiles react as interoperable values that can change their state according to the prevailing traffic behavioral pattern.

2.1.1. European applied connected car solutions

Connected Autonomous Vehicles

One of the earliest autonomous vehicle (AV) systems has been active from 1999 in a business park in Rivium (Netherlands) [4]. It consisted of a dedicated 1800m track, 8 stations, 6 crossings for traffic and pedestrians and 6 electric vehicles. The max number of daily passengers served, was around 3500 with a peak capacity of 500 individuals per hour and the average route duration around 2.5 minutes. A Personal Rapid Transit (PRT) system has been servicing a 1.9km point-to-point guided track between Terminal 5 and a Business Car Park at Heathrow with 21 vehicles. The system has carried 700,000 passengers with 99.7% system availability. Heathrow PRT makes more than 70,000 bus journeys off the road per year, saving more than 200 metric tons of CO_2 per year and is currently completing more than 5000 journeys per week.

CityMobil2

A very interesting project took place in 2012, by the Center of Transport and Logistics in Italy [4]. CityMobil2, which initially included advanced functions and set up a pilot platform for automated road transport systems (ARTS), was developed as a rethinking of mobility, mainly in cities and urban environments across Europe.

CityMobil2 is establishing pilot platforms for automated road transportation systems. These systems are steadily installed in many urban locations across Europe. They operate with driverless vehicles, executing routes in collective mode. They are deemed to play a useful role in the transport mix as they can supply a good transport service (individual or massive) in areas of low or dispersed demand, expanding this way the main public transport network.

Many local authorities were eligible to be one of the five sites to host a 6-month experimental transportation application. All authorities recognize the potential of vehicle automation as part of their public transport network among with the efficiency and cost saving opportunities offered by this implementation. The legal issues surrounding automated transport is another major concern to be addressed later, leading to a proposed framework for certifying automated transport systems.

CityMobil2 started in September 2012 and successfully ended in August 2016 including multiple collaborations with suppliers, city authorities (and local partners), the research community and networking organizations. It was founded by the European Commission. ERTICO (European Road Transport Telematics Implementation Coordination) is now leading the legal authorization and certification framework of the automated vehicles.

Smart Parking & Smart Lighting

The first ever city to run through a pilot smart city application in Greece, Chalkida [5], was selected, offering the opportunity to export useful data & application results in real life traffic management.

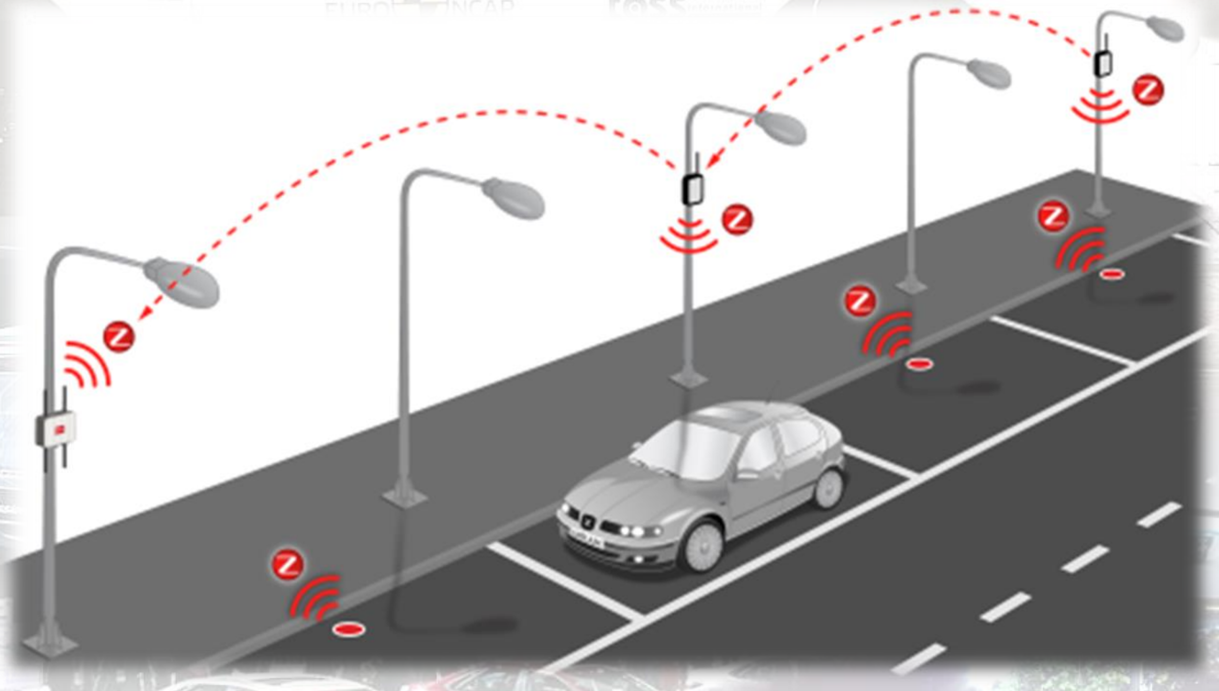


Image 7: *The Smart Parking and Smart Lighting application, as an urban connectivity infrastructure (lifo.gr, 2016)* [8]

The project started in the fourth quarter of 2016 and included Smart Parking platforms and Smart Lighting through the city. It is entirely supported by COSMOTE S.A, the major telecommunications vendor of Greece. Those two applications offer significant urban support, as they were initially developed, utilized and integrated into one common Smart City Synergy Platform.

Smart Lighting, the second part of this project, includes active adjustable lighting equipment. Through smart sensors, scattered around the city, the emitting motorway light signals detect the current ambient LUX, providing this way, automated adaptive control of the highway luminosity, even in a foggy or cloudy daylight. As a result, the system provides clever electricity management and adaptive motorway lighting. The estimated power efficiency is very promising, reaching about 60% less electricity consumption [5], as LEDs replace the traditional light bulbs on every pillar.

Both applications lead to a smart city integration through urban environment, by adopting smart technologies that can easily correlate with the upcoming Internet of Things. The current project is still in progress and sponsored by two other parties, Cisco Systems Hellas™ and Kafkas LLC.

Cooperative Intelligent Transport System

The C-ITS is a project adopted by the European Commission on November 2016, on behalf of the infrastructure deployment plans on EU roads, that will go live in 2019 [6]. The respective system is designed to supply vehicles and drivers with additional hidden info, as well as active management between different vehicles when located on close range. The extended system is coordinated by over the air transmission of information, by briefing drivers and passengers with useful notifications like imminent collision, icy road, heavy traffic congestion and surrounding vehicular “behavior”.

In addition, the vehicles involved in a possible incident are automatically alerted with wireless mechanisms, as to proactively avoid unwanted conditions or threats, like pedestrian crossing and challenging weather conditions by either automated braking or by automatically selecting driving modes for manual driving assistance.

The feature of nearby wireless handshake of transportation vessels is expected to expand the market potential of cooperative, connected and automated driving around the EU grounds. The key to this application is the processing of scattered data received from other devices to generate predictive warnings, tactical advices and useful driver information.

Image 8: ***A mere representation of the C-ITS platform, operating as an active urban eco-system*** *(autotalk.com, 2016)*[9]

Close passing-by vehicles, no matter what their direction, according to this platform, are continuously broadcasting data communicating their current position, actual speed, driving direction and real-time information, such as an obstacle at a certain road segment. Similarly, in cases of difficult weather or environment difficulties, the units propagate messages, such as speed limit and traffic lights sync information.

Furthermore, through the vehicular sensors, a few other services are supported, such as collision detection alarms and predictive road monitoring for maximum accident avoidance in certain regional areas with snow, fog or slippery tarmac.

The great concern was rotated around the limited modern motorways improvement measures the governments could enforce, as safety was mostly focused on vehicle equipment and crash tolerance and less on road management and smart transportation technologies.

The C-ITS platform will be provisioned as one of the most important milestones in the car history, creating further expectations for the markets, such as economic advantages, a new approach in the car market and proper correlation of information technology and vehicles. The most important factor for a promising C-ITS network will be the massive elimination of fatal accidents in EU, targeting almost half of today's official filed cases.

2.1.2. American Connected Vehicle Projects

US Department of Transportation Connected Vehicle Pilot Deployment Program

The U.S. Department of Transportation's (USDOT's) connected vehicle program focused on a deep research in order to run connectivity scenarios among vehicles and infrastructures while evaluating security in wireless devices. The project team selected special road infrastructure equipment, applied on motorway and urban transportation [7], as an initiative to minimize pollution factors and provide a safer car management system. Both prototypes and experimental concepts were applied in different locations in the U.S..

The National Highway Traffic Safety Administration (NHTSA) based its actions on the CV research program, embedded V2V communications technologies for civilian vehicles, continuing this way the Connected Vehicle Pilot Deployment Program. The last one consisted of three main parties, working on a 20-month phase of CV testing, including mobile transmissions, RSU (Road Side Units) architectures and public motorways tech-planning. Supposedly, the modern lifestyle people follow in Western Europe for the last 20 years has brought up a growing demand for a combination of personal transportation and social networking.

Good examples, depicting this trend, are Uber Taxi Service and Taxibeat applications, who support thousands users on daily requests. Services such as these, offer on demand transportation with taxi cabs, between any locations, through a connected platform. Under cloud infrastructures and dense databases, users who have downloaded the proper smartphone application on their handhelds, can "call" a taxi from their location, via the shared GPS and location data.

The specific service providers offer short or long distance transportation via an expanded platform, by accessing client-server locations while exporting estimated trip duration for every route. All of this information is instantly displayed on end-users' mobile phone screens, in just a few seconds. Techniques of that kind offer a wide range of social internetworking abilities for transportation purposes, limiting awaiting times and serving consequent users with minimum dead time.

Paramics API

Paramics developed an application programming interface that could actually map vehicle connectivity. Any vehicle-to-vehicle communication is compiled based on dynamic route guidance. This feature supplies connected vehicles with direct connectivity pairing without the requirement of any 3rd party networking infrastructure between them. In other words, the certain API offers a sustainable wireless handshaking session between moving cars.

The dynamic route guidance allows each equipped vehicle to update the routing table, stored in the access memory of their dedicated chipsets. The info collected and processed is essential for routing-guidance and direction alteration and operates just like xDSL nodes, between short-range vehicles. Vehicles that carry important data are selected to transmit their “info-tables” to the rest who haven’t obtained that yet.

The application relies on the length and speed limit of each info-exchange action. While other connectivity systems require one or more access points through the transmission medium, the specific API diagnoses each car’s vehicular route in addition to the other passing-by vehicles around, in order to successfully aggregate the collected information. The travelling times, are estimated according to each vehicle speed and user-defined range, for a guaranteed data distribution across end-users, similarly to the platooning procedure [7].

The data table only holds recent information around other vehicles, providing almost real-time feedback. The dedicated short range communication technology (DSRC) is set at approximately 1000m, but can be adjusted automatically to receive info effortlessly in shorter or longer distances and via various communication technologies. The rated information is sorted and selected for deciding the quickest path available to the final destination. The API is also user-defined, meaning the dedicated driver preferences for each route.

All connected vehicles that follow this rule, will always follow the quickest path given to them by their up-to-date trip table. This eliminates traffic congestions, reduces fuel consumption and records the desirable route in advance, when possible.

Connected vehicles with the Paramics API, are expected to not only calculate the estimated time of arrival (ETA) by GPS and current vehicular speed. Instead, they have the ability to predict the travel time for the entire route, seamlessly. Eventually, all cars equipped with this technology will ensure their drivers select the best routes possible and the traffic flows will coexist under a structured routing management.

2.2. User Experience Analysis of the Infotainment Systems

Ambient Technology in Vehicles

A dedicated questionnaire was performed by two computer science analysts, Ahmad Bennakhi and Maytham Safar, in order to extract useful information over the in-car behavior of drivers while interacting with their smartphones. The participants were all living in big cities and were all using their cars for their daily transportation [1]. The main goal of the survey was to define if the drivers were actually aware of the communication technologies around modern vehicles as well as the adoption rate of them by the users, for safety reasons.

The age group that participated the most, ranged from 25 to 64 years old, specifically the 45 to 54 years old age group had the most participation from the group that was previously specified. The biggest part consisted of people with high education and general knowledge over trending technologies.

More than half of the surveyed users stated that they often grab their phones while driving (52%), which depicts the exact ratio match to the portion of users that answer calls in most countries. Of the people surveyed, 63% reported that they text when driving. 44% of the total surveyed reported that they do it as common as at least once a week.

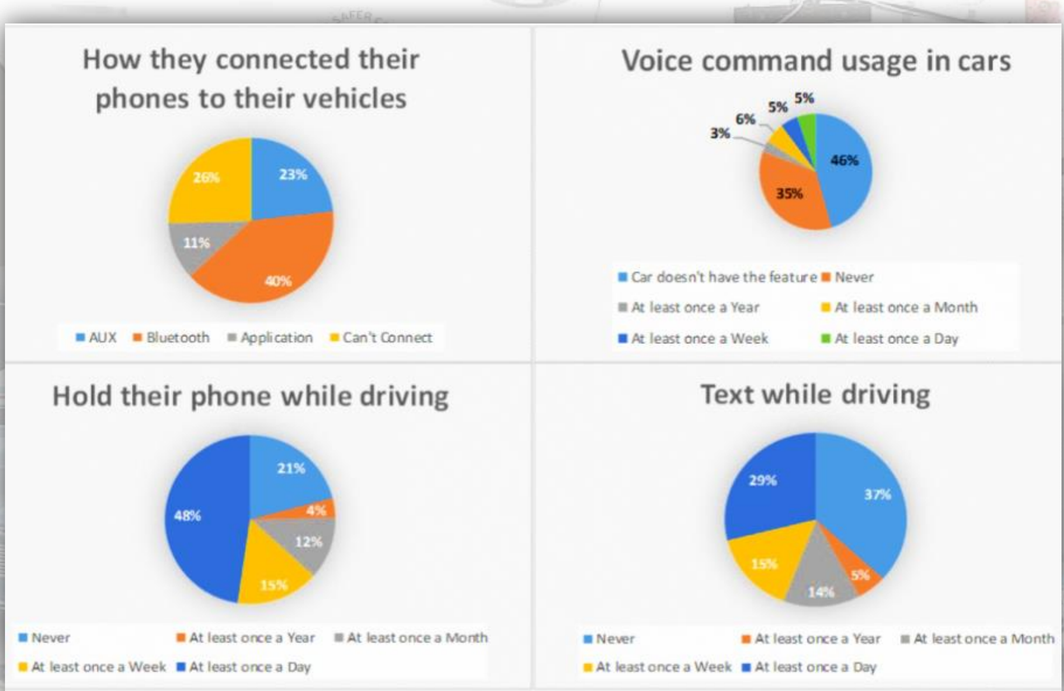


Figure 1: ***Statistic sample of actions executed by drivers while interacting with their handset onboard*** *(Procedia C.S., 2016)* [10]

After analyzing the survey results, many key points were revealed, following below:

- Most of the participants, who had voice command functionalities in their vehicles, weren’t actually willing to use it while driving. They were neither familiar nor used to operate this functionality on the road.

- A lot of them found it more practical to utilize the Text-to-Voice feature (38%) in their smartphones rather than using the Voice-to-Text feature (25%).

- The most preferable connectivity between smartphone and car was via the Bluetooth suite (54%). Second was via built-in applications (15%) and last via the auxiliary output (AUX) (31%).

- There was a great part of the surveyed people that never actually used a smartphone assistant such as Siri or Cortana (69%), although they were aware of their existence in their devices.

- The participants who occasionally used any voice command feature were not of a significant amount, but they were more than willing to text while on the steering wheel.

- A great part of the surveyed participants either text while driving, at least once every day (29%), while others never attempted to do that (37%). The rest of the sample did it, but less frequently.

Other than that, the final results of the survey, previewed that even though embedded applications were installed in vehicles, the habit of texting while driving was never gone, for most of the participants.

The older part of the sample was not keen on texting while on the road, but drivers aged 18 to 24 were among those who did it most frequently. Conclusively, despite the available car applications for communication purposes, the overall driving behavior was not adapted to them [1]. As a result, these applications were only faced as secondary communication tools for many drivers.

Current technologies had minor or no effect at all, as young people seem to choose their handheld devices for regular texting or chatting applications, such as Facebook Live, Viber or Skype. The late trends and the smartphone adoption made it clear enough, that age is the major factor when it comes to adopting new methods of communication.

The ambient car factors

In order to determine the contributing factors to the unexpected increase in the average travel time, test networks were set up and different factors were varied.

These factors are [8]:

- Network complexity
- Number of lanes
- Demand level
- Connected vehicle market penetration

The flow throughout the motorway network is applied in various market penetration levels of connected vehicles, starting from civilian ordinary vehicles to professional transportation truck fleet systems. Developing CV principles is a difficult part of the big project, as universal applicability is demanded on every functional level.

Until 2012, no significant technologic changes happened within the automobile industry for 15 consecutive years. 2012 was the year that marked a valuable checkpoint, from which numerous innovative opportunities emerged.

Tesla was among the first corporations to shape an advanced application interface that could establish a cloud-based connectivity, able to access remote vehicular or traffic data and receive system updates with modern OTA-wireless procedures. Ever since the experimental prototype vehicles from Google, initially across America, the automotive market's tensions were significantly affected, leading to next generation car connectivity solutions.

Since last year, many technology vendors (most of them originated from China), have produced On Board Diagnostic devices that can support telematics and car applications, providing drivers with a removable reporting mechanism for their legacy vehicles. OBD devices operate under Bluetooth low energy (BLE) protocols, offering audio feedback for effective tips while driving, through an Android - based internet platform.

By registering a vehicle through the serial port, a secured car connection is established between it and the user's smartphone, providing essential information over road incidents, navigation and mechanical status. This scheme offers a user-friendly in-car experience, without significantly alternating the vehicle’s interior.

Image 9: *Tesla Model X, the first electric car to have OTA technology on its main console (money.cnn.com, 2016)*[11]

Image 10: *AutomaticLink (left) and Intel on board diagnostics units, compatible with legacy vehicles, through the dedicated DIN slots (hardwarezone.com, 2016)*[12]

Both new firms and legacy companies are competing in this new market opportunity with promising business models, providing a primordial legacy to connected car transformation in the modern life.

A lot of new and older tech parties have shaped alliance, predicting the increasing car industry formation, offering certain telematics and connectivity solutions that can be industrially or manually applied on compatible vehicles of this kind.

Some of them are already integrated into production lines, while others are mainly researching and developing standalone 3rd party accessories and services, like add-ons, safety mechanisms, peripheral connectivity and advanced car diagnostics.

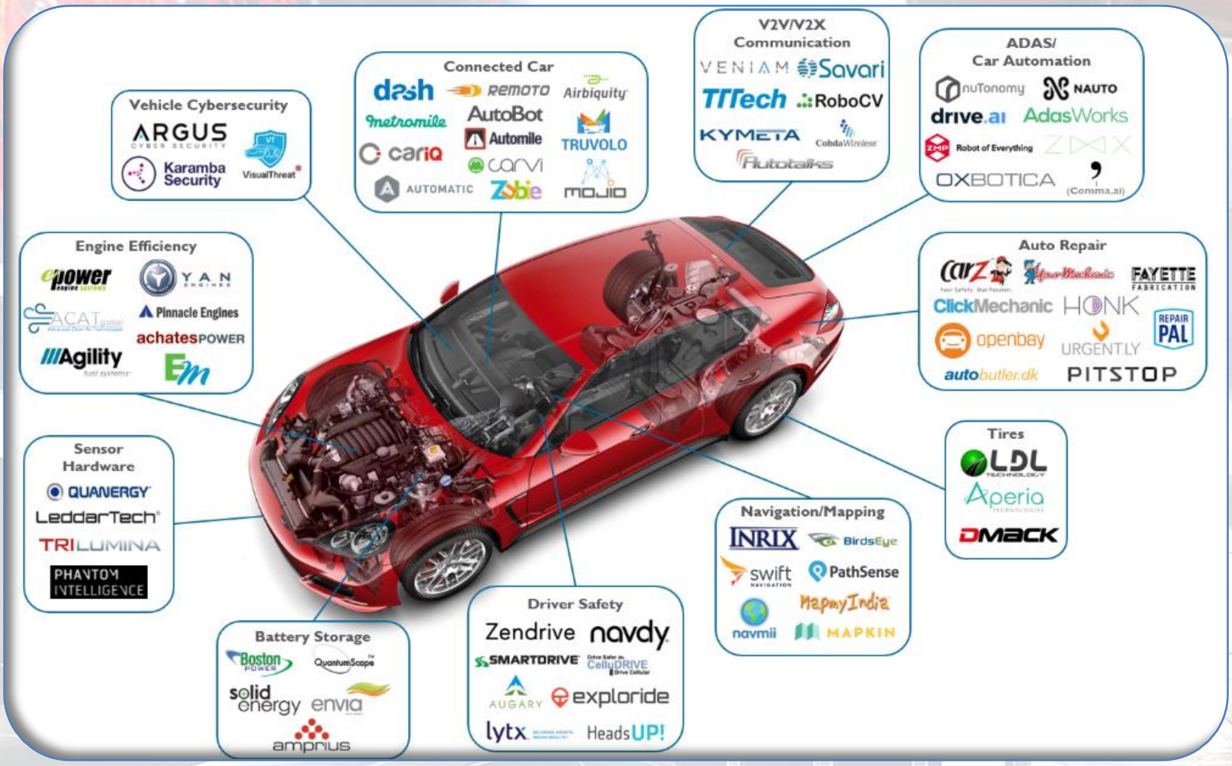


Image 11: *Some of the market's leading automotive technology companies, ready to provide advanced solutions to the V2V & V2X environment, offering complete vehicle connectivity (cbinsights.com, 2016)* [13]

On the other hand, IBM developed a single, vivid multi-layer connected car environment that is supported by numerous applications and services, proving the extended efficiency of a multi-layer connectivity, as the one demonstrated below:

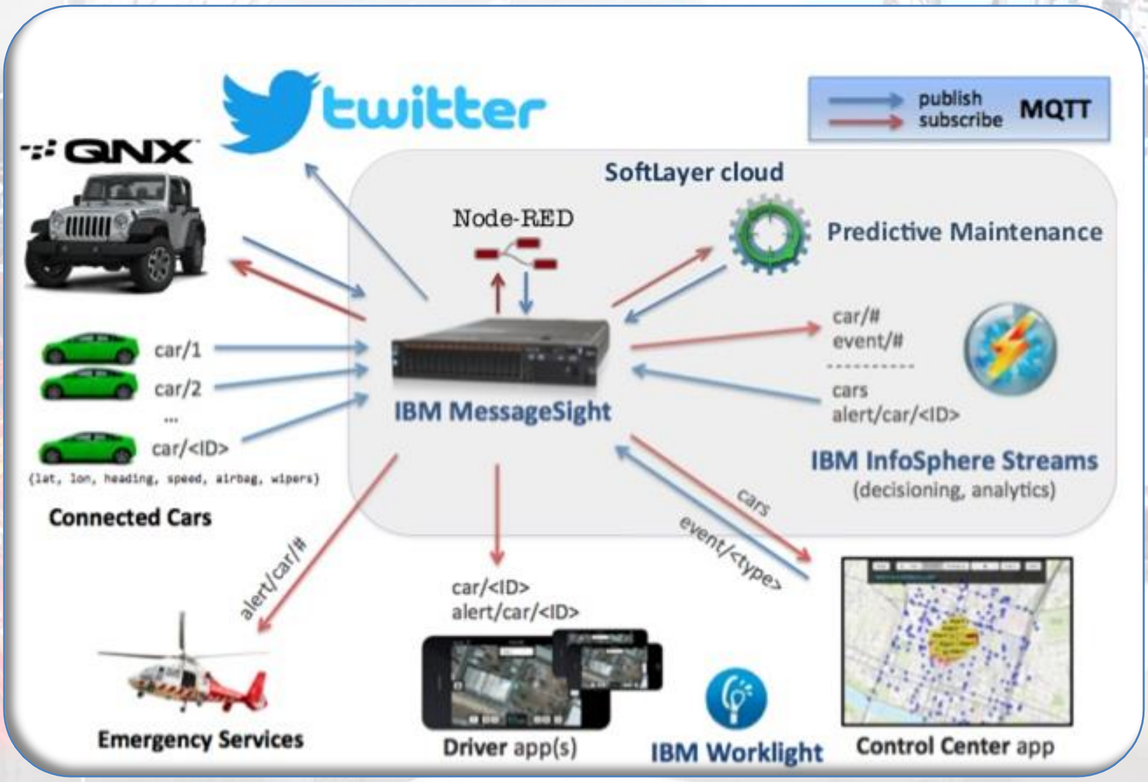


Image 12: *The IBM Connected car platform supports applications, services, location, cloud databases and predictive intelligence among vehicles, through the IBM MessageSight* (connected-car.mybluemix.net, 2016) [14]

The IBM C2x (Car-2-x) architecture combines vehicle monitoring, security and data services. It utilizes data generated from vehicles, devices and systems into an integrated digital platform to enable a range of innovative solutions that enhance safety and traffic assistance. Using a big data and analytics platform, based on open standards, along with cloud and mobile technologies, new services and business models can support driver provisioning with the same connectivity, interactivity, personalization and intelligence, users have come to expect from any other smart devices.

The collection and analysis of large data flows of vehicular and repair data leads to gathered info, used to export predictive results in order to prevent problems before they end up in any mechanical failure. IBM's major concern about the generated information, is the hidden meaning behind it, could exclusively emerge when data are applied to predictive analytics and vehicle telematics systems, as only then is it plausible to identify problems more quickly, reduce unplanned maintenance, improve customer service, lower warranty costs through more accurate diagnoses and offer diagnostic services tailored to each vehicle/owner.

As mentioned earlier, the future vehicular transportation will be supervised and controlled in general, by telematics and information technology. In 2013 Machina Research predicted that by 2020, 90 percent of new cars will feature a built-in connectivity platform, as the connectivity of vehicles is the key to unlocking mobility features and full compatibility.

Car maintenance

Another great concern, future connected car buyers are concerned, is the overall financial maintenance of their vehicle. By the time wireless and embedded applications are about to be integrated into vehicles, many people have expressed their inquiries over the budget that shall be needed in order to keep their connected car around.

The McKinsey & Company consulting group, dealt with plenty of data and marketing information in order to edit an -as accurate as possible- estimation over the tension of the future car ownership total cost. Surprisingly it seems like it will remain stable for consumers but the dramatic increase in vehicle connectivity around the globe will chain effect the value of the global market for connectivity aftermarket components and services to €170 billion by 2020 from today's €30 billion.

While technological advances have driven the automotive sector for decades, this dramatic acceleration (as a result of connectivity) offers the potential to significantly alter the competitive landscape. Companies from the software and telecommunications sectors are already entering the automotive market and one of McKinsey's reports, finds that original-equipment manufacturers need to act now to take advantage of today's connection deployment, as such actions would evade competitive -below the belt- hits from other automotive-software team-ups.

2.2.1. In-car Commercial Solutions

Voice Recognition Support

In 2017, voice recognition features are integrated into many flagship models, but so far, only few of them are upgraded enough to approach the human behavior and let drivers completely rely on them. Voice call activation, driving modes, electronic seat settings and even online emergency systems, are some of the modern integrations in the car market. What car makers really look for is developing an empathic vehicular environment, where key phrases can activate the essential car functionalities and cabin crew motions can be recognized and handled with care.

Some really good future scenarios, rather user-friendly for all passengers (including the driver), reproduce an AI mechanism, that can track vital signs of individuals inside the car. Indications of physical fatigue or stress (anger, weakness or nausea) could easily be vanished, by having the car relax the driver with simple methods, like soft-music auto tuning, or air ventilation adjustment [1]. Moreover, any vital-abnormalities such as strokes or heart attacks are extremely hazardous, as there are numerous recorded cases where vehicles ended up in fatal crashes, after the drivers felt unconscious or faced seizures, losing the control. Even if these services were leased, a lot of conscientious drivers would pay that extra money to obtain significant services of that kind.

Even if car companies, equip vehicles with voice recognition technology, this service is still not 100% reliable. The algorithms applied cannot always recognize the user requests, either due to voice frequencies or when ambient surrounding noise disrupts the voice detection. Nowadays it is more common to apply cloud based applications for voice recognition features, but until now this is also a very difficult implementation.

Cars and vehicles in general are not yet “connected” and cloud based features need connectivity and cellular data contracts [1] that are quite costly for smartphone applications. Another problem here is that standalone systems are more processing efficient than cloud based ones (which usually need some loading time). Unavoidably, both methods seem to encounter the same problem of filtering out the background noise that cars are mostly known for, such as the A/C fan, high engine RPMs and external surrounding noise.

Bright HD displays are quite helpful inside vehicles. Good examples would be Tesla’s main console and Audi’s new media center. This all is no secret, but what car manufacturers are interested in, is providing advanced solutions, enhancing the in-car experience and making cars safer than ever. That is, minimizing distractions and easing the driver with minimum gesture requirements.

The voice recognition feature could also apply on numerous other cases and functionalities. Turning the car's main console into a media station with a computer interface provides a better user-experience and multiple ways of activating or deactivating systems, either by hand, or vocally. Above all, the target is to implement such features in a way that users will be more willing to adjust their driving profile accordingly.

Once again, such systems are still prone to be hacked, or overridden by remote attackers. Speaking of security, cars with advanced console systems are significantly more vulnerable and rather exposed to any close range network transmission. It should be taken for granted, that such systems could support driver alert mechanisms, in cases of any hacking attacks. But the truth is that no such mechanisms exist yet and there are always threats, aiming either for the vehicle's control or the car microphone's access.

Note that, for most modern cars, their console remains one of the greatest security breaches, but only a few are aware of that. The misconception of the vehicle's total ambient isolation is always around, especially since people are not aware of the dangers and capabilities of technology.

The same thing happens with mobile devices such as smartphones, where security gaps may occur towards applications installed on it, in addition to the network trustworthiness under which these devices operate. As it is going to be discussed on a later section, new security policies and issues arise, along with legal regulations and restrictions that could threaten the public transportation in general.

Auto Pilot Systems

Over the past few years, the automotive industries transformed their regular production line vehicles into multimedia systems able to transport people, among other functions. In just a few years the auto-pilot system showed up as a developing project, ready to go live before 2020.

Image 13: ***Audi's one of the very first attempts to engage motorways with auto-piloted vehicles, came through with the A7 series model, initially tested and developed in the U.S.*** *(slashgear.com, 2015)* [15]

Autonomous vehicles (AVs) have been around as of April 2014 with Google cars literally scanning the whole world. The automated systems Google used in many car manufacturers (Volvo, Ford, BMW, Cadillac, Mercedes-Benz etc.), managed to record and visualize the Google maps, by offering the famous Google Street View.

By computerizing functions and procedures in motherboard chipsets, the newest car models include rich automated features such as adaptive cruise control and parking assist systems that allow them to steer themselves into parking spaces.

Some companies have already created state-of-art car systems, by entirely developing and programming AVs that can drive themselves on existing roads and can navigate many types of road terrains with almost no direct human intervention.

Image 14: *Lexus RX 450h, one of Google's self-driving vehicles, used in digital "capturing" of highway and urban routes around regions, enhancing Google Maps with the recent Street View feature* (forbes.com, 2016) [16]

Assuming these technologies become successful and available to the mass market, AVs will soon take their chances on dramatically changing the transportation network. The most complex part is that of the policymakers as it will be discussed further in detail.

AVs have the potential to fundamentally alter transportation systems by averting deadly crashes, providing critical mobility to the elderly and disabled, increasing road capacity, saving fuel and minimizing CO_2 emissions. Complementary trends in shared rides and vehicles may lead vehicles ending up from an owned product to an on-demand service.

Infrastructure investments and operational improvements, travel preferences and parking needs, land use patterns, trucking and other activities may be affected. Additionally, the passenger cabin may be transformed in a way to help former drivers spend more time on their laptops, for food consumption, entertainment (watching movies, music) and calling others, safely.

Potentials of the AVs can easily be compared to today's transportation means and routes. Two automotive researchers, Daniel J. Fagnant & Kara Kockelman [9], revealed all opportunities, barriers and policy recommendations that would eventually transform the future human transportation into a self-driving network, possible to be requested on-demand at any moment and by anyone.

Those potentials are predicted to immediately affect the following aspects of today's life:

- ✓ **Changes in Vehicle Miles Travelled (VMT) and vehicle ownership**
- ✓ **Discount rate & technology costs**
- ✓ **Enhanced safety specifications**
- ✓ **Congestion Reduction**
- ✓ **Parking efficiency**
- ✓ **Economic impacts**

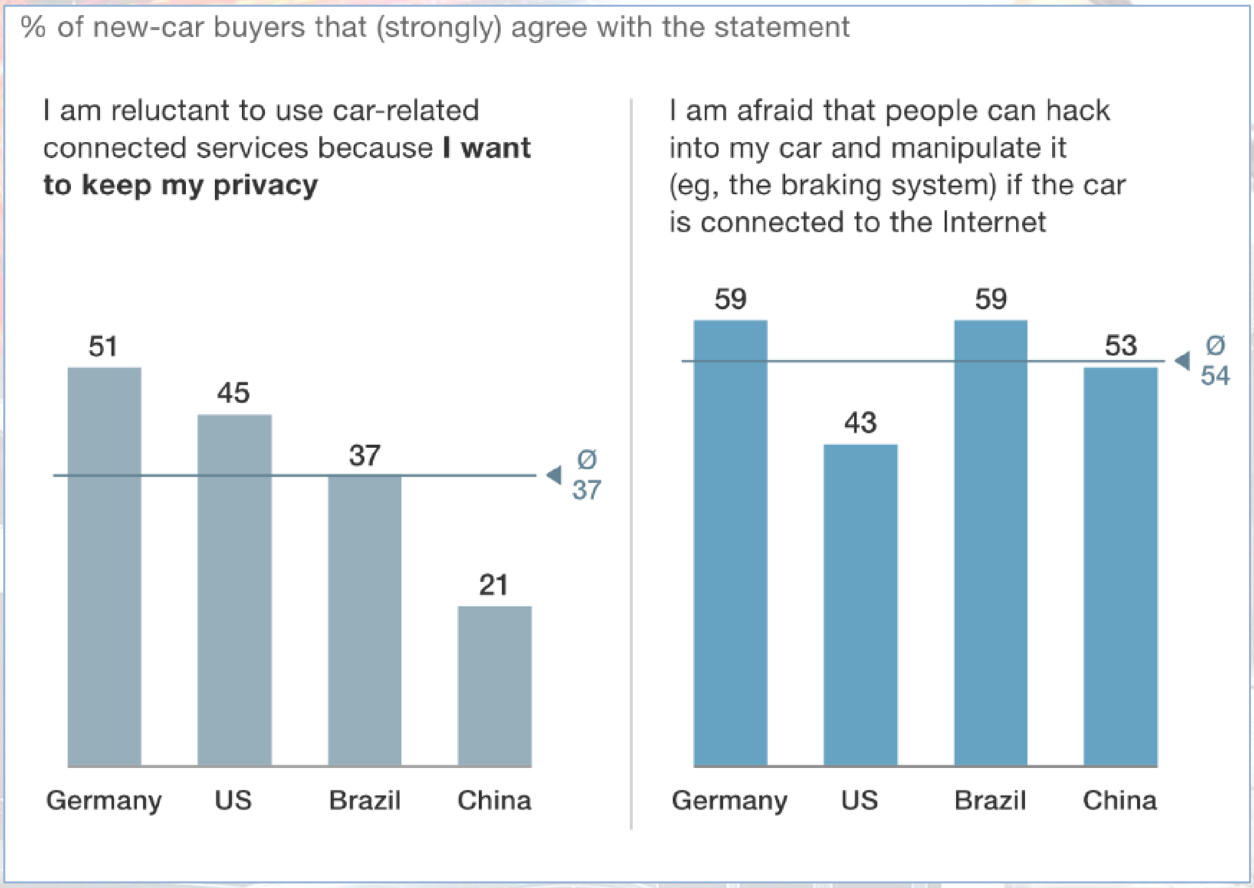
Considering the fact that autonomous vehicles could only positively affect every person's life, Fagnant & Kockelman gathered and examined all values, in order to extract a precise rate of development for each of those aspects.

2.2.2. Efficiency & Driving Modes

Potential buyers of connected vehicles are probably going to think more than twice before ending up with a manufacturer agreement. Although the automotive industry promises plenty of assistive systems for their latest models, a great part of drivers still insist, the overall control of a vehicle should be mostly managed by the driver and not via ECUs, smart systems or artificial intelligence.

A prevailing opinion goes through everyone's mind, putting aside any electronic systems that can sustain auto-piloted modes. New car buyers are broadly concerned about data privacy and the possibility of hacking when it comes to vehicle connectivity.

The probable failure of full auto-assisted systems brings fear of complete control loss in case of an emergency or system malfunction. Other than that, security and hacking scenarios lead to precariousness and lack of motivation for a great part of car buyers. That regional variation is lower than the first buyers' part, however, when it comes to fears about vehicles being hacked, significant concerns [10] are evident in all markets.



Graph 1: ***Security and privacy concerns over connected vehicles, according to a McKinsey Consumer Survey*** *(mckinsey.com, 2014)* [17]

It seems that car manufacturers who join software and hardware IT developers, need to convince their dedicated market groups, by assuring them of end-to-end reliability and trustworthiness for their integrated driving systems. Of course that demands multiple simulations and on-road testing with tangible facts.

During these systems development, car makers started thinking of advanced adaptive equipment, in order to slowly prepare the market for fully auto-piloted vehicles. This is a sign that self-driving vehicles will not emerge in the consumer market, at least not before they are applied and tested to industrial and corporate schemes, such as transportation trucks, modern agriculture, construction and manufacturing sites.

The following pattern, demonstrates some of the most ideal driving automation levels that could be applied in vehicles, based on driving modes, which can expand from driver aided assistance to full automation and control:

	SAE Level	Name	Steering, acceleration, deceleration	Monitoring driving environment	Fallback performance of dynamic driving task	System capability (driving modes)
Human monitors environment	0	**No automation** the full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems	👤	👤	👤	n/a
Human monitors environment	1	**Driver assistance** the driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task.	👤 🚗	👤	👤	Some driving modes
Human monitors environment	2	**Partial automation** the driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task	🚗	👤	👤	Some driving modes
Car monitors environment	3	**Conditional automation** the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene	🚗	🚗	👤	Some driving modes
Car monitors environment	4	**High automation** the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene	🚗	🚗	🚗	Some driving modes
Car monitors environment	5	**Full automation** the full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver	🚗	🚗	🚗	All driving modes

Table 2: *Weighted levels of driving modes for connected cars* (epthinktank.eu, 2016) [18]

Speaking of autonomous connected vehicles, up to this day, many reported cases have revealed issues, originated from possible connectivity or processing malfunctions, able to cause from minor crash accidents to even fatal ones.

On May 2016, Tesla Motors faced a serious accident located in China, involving one of its flagship models, the Tesla Model S. The driver was at that time resting on the driver's seat, with the autopilot enabled during his last trip. For some reason, the autopilot wasn't able to engage the braking systems because the 'Traffic-Aware Cruise Control' didn't detect the oncoming obstacle on the driving lane it was located. The vehicle was running towards a street cleaning truck operating on the half of the driver's direction - lane.

The unlucky driver's family sued the company, hitting the blame on the Autopilot system, for having dysfunctional equipment loaded on the Tesla car and eventually "killing" the person inside. The vehicle was actually destroyed, the log transmission system broke down and didn't operate properly making it practically impossible to identify the reasons the accident wasn't avoided at that time. The only testimonial material available for further processing was the vehicle's dashboard camera, which recorded the high-speed crash showing the enabled autopilot feature on the main HUD.

Tesla immediately took awareness and liability over the incident, but reminded the audience and the news channels that the specific model was actually considered a Level 2 (Partial Automation) on NHTSA's 0-4 scale of autonomy, meaning the driver should still be aware of the surrounding motorway environment, as the system was on beta testing phase, unable to detect close calling obstacles under certain circumstances.

Image 15: *The Tesla Model S was involved in a critical high-speed collision, leading to a fatal crash. The driver, according to the manufacturer, wasn't aware of the truck that was operating on the half side of the vehicle's lane* (electrek.co, 2016)[19]

The official Tesla announcement, justifying the causes of the accident, stated that, there may be situations in which the Traffic-Aware Cruise Control may not always detect a vehicle, bicycle, or pedestrian. Depending exclusively on the Traffic-Aware Cruise Control to avoid a collision can result in serious injuries or even death. In the incident, Tesla says that Autopilot failed to see the white side of the truck against a brightly lit sky.

2.3. Case Studies of High-tech Transportation Patterns in Public Use

2.3.1. Case study of the State of Oregon, USA

The dedicated case study was initially intended to record opinions and facts, based on the connected and automated vehicles penetration, also categorizing the expectations of the relative U.S. Departments in Oregon. The main aspect of this effort was to write down the vision that was perceived from different stakeholders, such as local and transit agencies, the state authorities and many more, according to the future major connected vehicle deployment, on a metropolitan level [7].

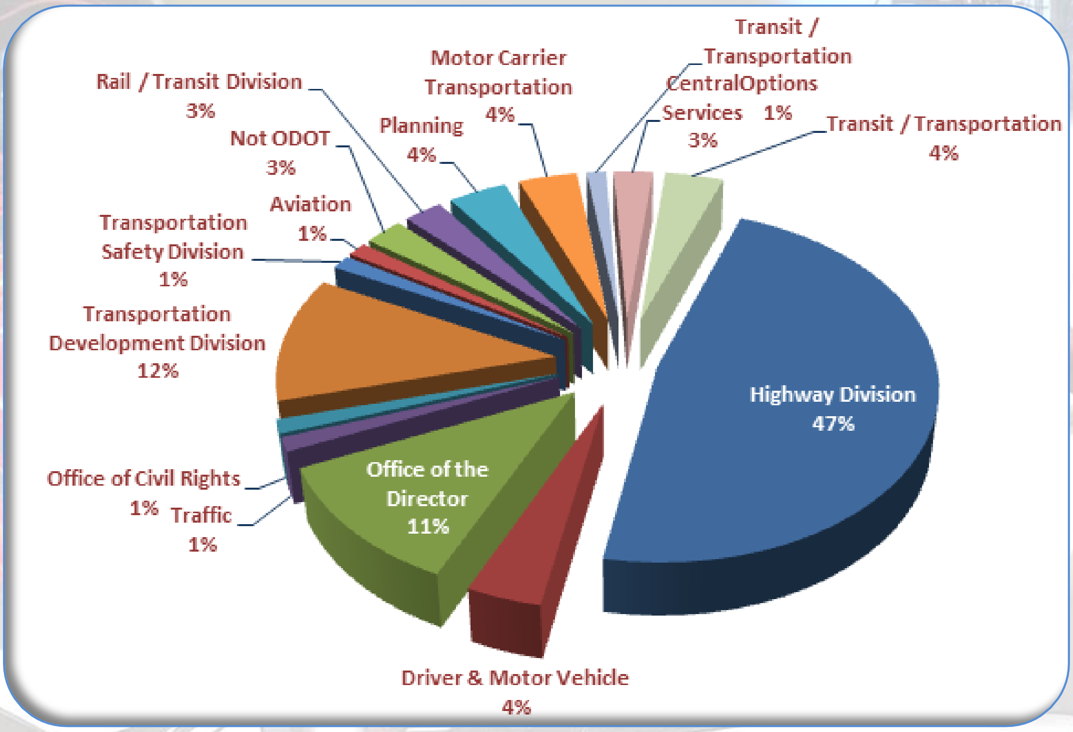
According to the study findings, of all the accidents issued in the U.S. annually (6 million on average), more than 32,000 fatal cases are filed, following no less than 2.2 million heavy injuries. The lack of safety measures, the inappropriate motorway elements, the urban congestion in most cities and the need for more energy consumption (petrol & diesel), are only few of the main reasons that burden the government and the highway transportation departments from establishing safe and secure transportation networks across states. The same obstacles seem to apply in Europe and other continents as well.

The U.S. Department of Transportation had scheduled major plans, to later develop connected vehicle safety mechanisms, applications and standards, using short-range wireless communications protocols. The DSRC technology can contribute in elaborating efficient wireless systems with OTA updates for vehicles in high speed.

A previous research issued by the NHTSA, verified a scheme – method through which around 80% of the non-fatal accidents could somehow proactively be avoided, utilizing real-time traffic management applications, tunneled through connected vehicle technology infrastructures.

Through the Safety Pilot Project that took place in Michigan (2012-2013), the US. DOT simulated real-world scenarios based on the effectiveness and response of wireless connected vehicle technology. They also tested multimodal adaptive driving cases, by collecting data from the drivers (sample) that participated. The exported safety specifications were really ambitious and the following results of the Oregon Research Program, charted an accurate ratio that demonstrated advantages and disadvantages among Connected Vehicles.

1) Below are the total survey respondents of the Oregon Department of Transportation (ODOT employees and external groups) [7]:



Graph 2: *The survey respondents, categorized as ODOT divisions (elsevier.com, 2016)* [20]

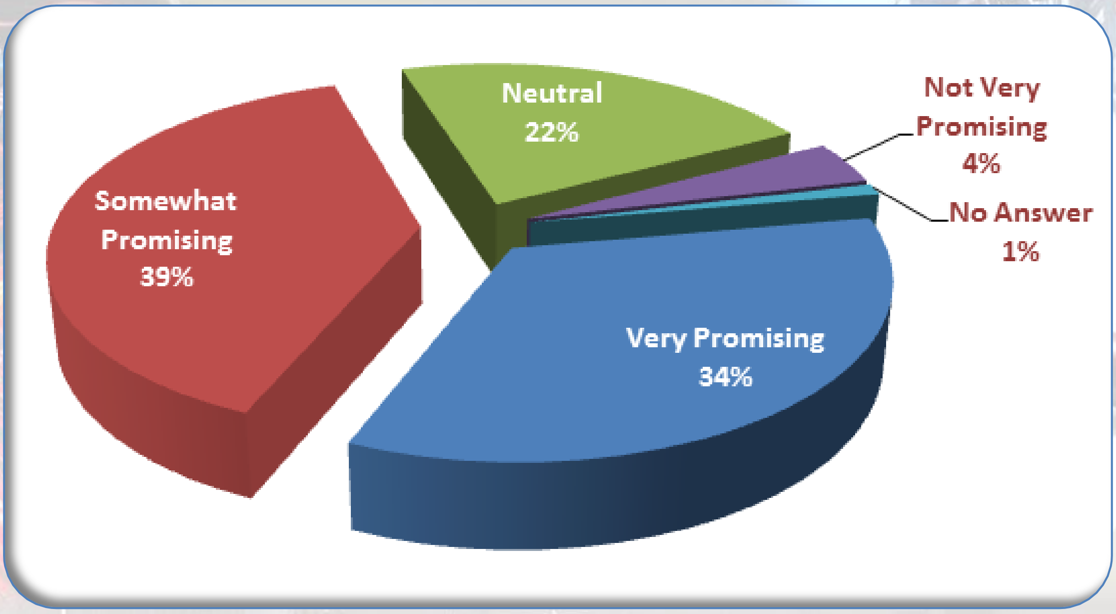
Only few participants of the surveyed sample (2%) were strictly negative in using connected cars [7]. Everyone was demanded to document an honest statement of what pros, cons, benefits and issues would occur if connected vehicles went live.

2) Benefits provided from connected vehicles, are listed as follow:

	Very Likely	Somewhat Likely	Somewhat Unlikely	Very Unlikely	No Answer
Reduced Crashes	55%	37%	5%	1%	2%
Reduced Crash Severity	48%	43%	6%	1%	2%
Improved Emergency Response	36%	50%	11%	1%	3%
Less Traffic Congestion	21%	46%	23%	7%	3%
Lower Vehicle Emissions	16%	47%	30%	5%	3%
Shorter Travel Times	17%	48%	30%	3%	3%
Better Fuel Economy	23%	57%	13%	3%	3%
Lower Insurance Rates	13%	40%	34%	10%	3%
Fewer Driver Distractions	11%	26%	38%	23%	2%
Improved Agency Operations	14%	48%	28%	5%	5%
Reduced Agency Costs	10%	30%	36%	19%	4%

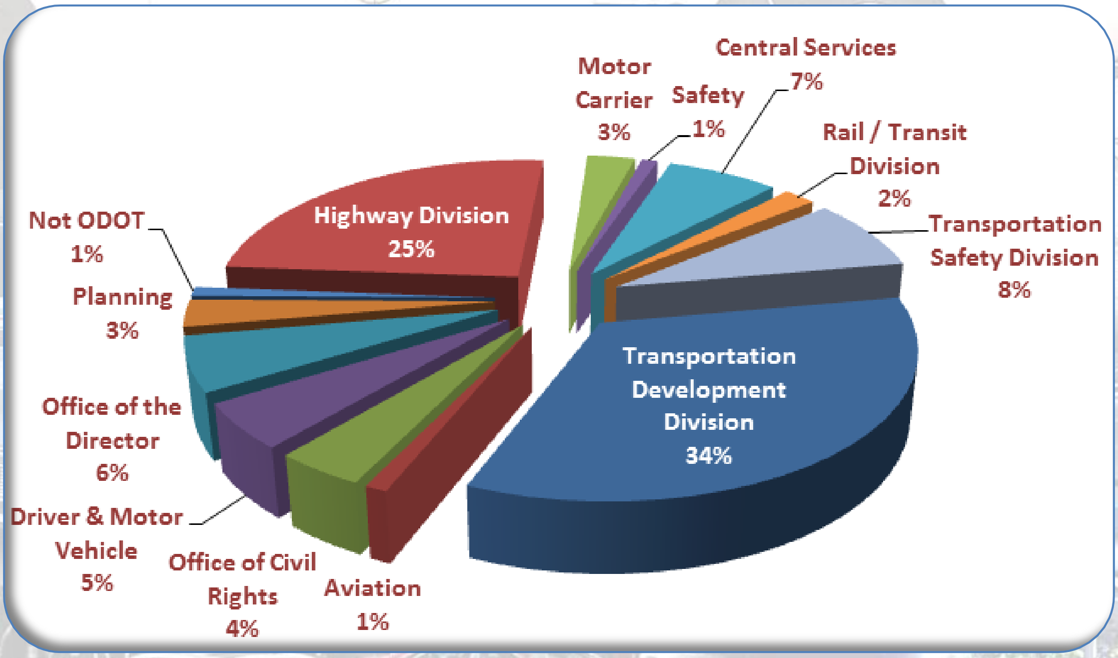
Table 3: *The estimated benefits of a CV environment, as documented from each division's aspect (elsevier.com, 2016)* [21]

3) The next graph gives a very trustworthy depiction of what the respondents believe, according to the deployment of Connected Vehicle Related Infrastructure:



Graph 3: ***Opinions about reliability of a CV deployed infrastructure, according to the submitted answers (elsevier.com, 2016)[22]***

4) The final chart qualifies the priorities, each division selected as the highest and most important parameters for a promising CV infrastructure development:



Graph 4: ***The final priority model, based on the answers provided by all divisions separately (elsevier.com, 2016)[23]***

Surprisingly, many of the respondents stated that they would expect a significant decrease in crashes and accidents, but a great part of them who weren't familiar with the modern technology were actually concerned about the effect of the new deployment. A great part of the first ones, would even trade personal user data in exchange for providing sufficient feedback for increasing safety on the roads. A lot of them claimed that automating vehicles by computerizing them with ECUs and OTA technologies would contribute the most, in minimizing accidents. The key point for the majority was the speed at which computers can respond and calculate, in contrast to the million times less responsive human reaction.

The results from the survey, revealed the confidence both ODOT and non ODOT's employees and divisions felt, regarding the technical readiness of the Transportation Department, over the connected vehicles in the next few years [7]. Some of them, expressed their concerns over the fact that their divisions are open to any innovation but suffer poor technical designing for the specific project. Time, cost, workload balancing and penetration rate are few of the limited profession issues over transforming the roads to software defined networks (SDNs).

Finally, the survey revealed that the ODOT was not (and would not yet be) prepared for a motorway implementation of that size. A lot of concerns were expressed, including state agencies that are -up to this day- famous for not being able to handle IT projects very well, compared to private parties who can manage milestones and project deliverables, much more effectively and on-time.

2.3.2. The Official VMT Percentage Analysis of the Texas Automotive Market

Fagnant and Kockelman, also ran a very fruitful marketing simulation of the future automotive penetration & congestion of connected cars in the Texan Market, Austin. According to the Vehicle Miles Travelled (VMT) per AV (autonomous vehicle), it was estimated that:

- AVs will have 20% higher VMT rate than non AVs, at a 10% market penetration level and
- 10% higher VMT rate at a 90% market penetration level

According to the estimated market reflection, it is expected for early adopters to be the first market share to trigger the demand of connected and autonomous vehicles. For the Texas market [9], a fleet of shared AVs serving over 56,000 trips a day was found to travel around 8.7% of its mileage unoccupied (empty). The percentage decreased to 4.5% when ride-sharing was permitted and minor (not more than 1%) net VMT reductions were realized when ride-sharing was permitted. On a first glance, the efficiency provided by ride-sharing mechanisms, tends to increase every time more data are broadcasted between routes and vehicles.

The analysis, through numerous simulations, also revealed that each AV could serve the same trip range as 10 civilian vehicles combined. Even though the 1 to 10 ratio was quite high for mass adoption in the automotive world, it was made clear that in the future, around half of all AV trips will be executed by shared AVs, while the rest of them will be served by personally-owned AVs. The above ratio is highly anticipated to apply best on long distance routes (more than 12 miles) and with low urban density. This is why AVs are expected to reduce crash and injury rates by 50% versus non-AVs at the 10% market penetration rate. Similarly, AVs are expected to be more than 90% safer than non-AVs at the 90% market penetration rate.

Pedestrian and bicycle crashes are also expected to partially experience AV safety benefits, but other means of transportation such as ATVs, trikes and motorbikes are not estimated to follow the autonomous driving modes soon enough. Especially for the two-wheel riders, currently around half of all fatal motorcycle crashes do not involve other vehicles, notifying that they will have to undergo a different technology and safety approach on a later implementation. Therefore motorbikes will only partially experience a decrease in their crash rates.

Average crash costs were also approached (ratio samples of filed crash incidents up to this day), with AVs to be a very promising deployment that shall among other, reduce the total damage cost [9] of each incident, once permitted. The table below demonstrates statistic approaches of fatal crashes occurred in the U.S. per year, on an average scale, while characterizing the causes of each incident:

U.S. crash motor vehicle scope and selected human and environmental factor involvement.

Total crashes per year in U.S. (Traffic Safety Facts, 2013)	5.5 million
% human cause as primary factor (National Highway Traffic Safety Administration, 2008)	93%
Economic costs of U.S. crashes (Blincoe et al, 2014)	$277 billion
% of U.S. GDP Blincoe et al, 2014; CIA, 2012	2%
Total fatal and injurious crashes per year in U.S. (Traffic Safety Facts, 2013)	2.22 million
Fatal crashes per year in U.S. (National Highway Traffic Safety Administration, 2012)	32,367
% of fatal crashes involving alcohol (National Highway Traffic Safety Administration, 2012)	31%
% involving speeding (National Highway Traffic Safety Administration, 2012)	30%
% involving distracted driver (National Highway Traffic Safety Administration, 2012)	21%
% involving failure to keep in proper lane (National Highway Traffic Safety Administration, 2012)	14%
% involving failure to yield right-of-way (National Highway Traffic Safety Administration, 2012)	11%
% involving wet road surface (National Highway Traffic Safety Administration, 2012)	11%
% involving erratic vehicle operation (National Highway Traffic Safety Administration, 2012)	9%
% involving inexperience or overcorrecting (National Highway Traffic Safety Administration, 2012)	8%
% involving drugs National Highway Traffic Safety Administration, 2012	7%
% involving ice, snow, debris, or other slippery surface (National Highway Traffic Safety Administration, 2012)	3.7%
% involving fatigued or sleeping driver (National Highway Traffic Safety Administration, 2012)	2.5%
% involving other prohibited driver errors (e.g. improper following, driving on shoulder, wrong side of road, improper turn, improper passing, etc.) (National Highway Traffic Safety Administration, 2012)	21%

Table 4: *Crash motor vehicle scope (avg. fatal crashes per annum in the U.S.)*
(elsevier.com, 2015) [24]

Over 40% of these fatal crashes included excessive alcohol consumption, some sort of weather or ambient distraction, drug involvement and/or even physical exhaustion [9]. Autonomous vehicles, according to digital systems engineers, would never lose their driving direction, provided that only minimal digital malfunctions would occur, while the whole in-car autopilot system would sustain its proper operation. Any driver error is believed to be the main reason behind over 90% of all crashes in total.

Harsh weather phenomena, like fog or snowstorms increase the collision possibilities, no matter what the sensors. AVs are still unable to overcome the majority of possible obstacles they have to face, due to the systems' limited scanning and identification power. Initially, pedestrians and medium sized objects have to be excluded from AVs' limited avoidance capabilities, as a measure to maintain public and private properties intact on similar cases.

Current systems of that kind are weak in perceptional scanning and decision making on the road. The human perception, response times and instant reactions are still the most safe and accurate. Liability for AV accidents is a major concern and could be the basic axis for future implementations.

Chapter 3rd

Telecom & Vehicle Convergence

3.1. The Rise of Telecom Services

Nowadays, everything is broadly related to mobile services, meaning that the most important features are the mobility and freedom the autonomous ICT systems offer, while being integrated in our lives. Surprisingly cars have been one of the latest yet updated targets of the automotive industry. The pace that is defined by all ICT vendors globally could not but include our everyday habits while merging mobile integration and services interaction, on the way to ease our daily tasks – chores – routines.

3.1.1. Modern telecom coverage and issues

The technological component of a CV requires a robust and steady platform that allows not only for creativity and interoperability, but also the ability to interact instantly and with full compatibility to the complex human behavior. This has become a cutting-edge area of research for more advanced and low cost intelligent transportation systems (ITS), as new Artificial Intelligence (AI) techniques are being aroused.

The latest traffic information systems are established upon a node communication model, with all the data aggregated in certain checkpoints (processing units) and the useful info broadcasted back to drivers. This method is not as accurate as needed, due to information delay times of collection and redistribution between broadcast points and end-users. That being said, it is also cost absorbing, considering the augmented infrastructure budget required. This has given rise to an increasing interest in computing and wireless communication in roadway transportation systems.

The expanding telecom coverage and compatibility between countries & continents (data-roaming discharge, 4G, LTE & 5G technologies) equips vehicles with processing power and strong, effective distance telecommunication mechanisms. For instance, the U.S. Federal Communications Commissions (FCC) allocated seven channels in the 5.9 GHZ band, allowed only for DSRC based services, regulated to support the V2V applications, available since 2010.

Comparing the legacy traffic information systems (RSS feed, radio news, roadwork services phone lines, RFID sensors etc.) with the V2V systems, the second ones offer the ability to create intermediate connections (ad-hoc), able to send and receive messages directly between two connected units. The Vehicle Ad-hoc Network (VANET) establishes pure wireless communication bridges between sequential vehicles that operate as repeaters, transferring the info to the final recipient.

Still, even though connectivity proves vital for a system of that kind to operate seamlessly, a lot of connectivity issues may emerge, as always happens with telecom services. Compatibility between different units, protocols routing, network capacity and delivery / response delay are few of the problems to be solved before any deployment.

A successful inter-vehicle communication (IVC), as defined by experts and automotive researchers, must operate under a guaranteed network transmission with extended 100% signal coverage, between all CVs on the local road network and only a drastically increased failure tolerance. Separately, the two conditions, an ideal IVC system is based upon, are:

- Those related to the traffic stream, such as traffic flow (density) and automotive market penetration

- Those related to the technology itself such as the transmission range, interference caused by the current infrastructures, the active environmental alterations (rain of fog attenuation) and channel information

Generally, a larger transmission range with higher traffic density and higher market penetration, allow more vehicles to be connected and information to propagate further on road networks. With all these factors, a measure of effectiveness can give an indicator for the performance of CV environments and account for as many of these factors as possible needed.

Nowadays, telecom vendors control the wireless coverage demand with the latest 4G, LTE & 5G technologies, similarly to cellular services. The initial idea of visualizing connected vehicles as a new profitability source was the first spark in attracting technology giants like Google, Apple & Tesla next to car manufacturers and telecom operators. It was the only missing part from the automotive industry and financial analysts predict a profitability indication of approximately $152 billion by the year 2020 around market shares in the future.

3.1.2. How Telecom Operators visualize their capital growth On the Connected Car Industry

On average drivers spend a third of their day driving their cars and in the next couple years, most new cars sold around the globe will have onboard digital connectivity as standard equipment. Digital technology means information & telecommunication services and telecom vendors are quite aware how to promote their services on digital platforms. The capitalization of vendors is expected to grow big and great telecommunication deployments are about to be released, considering the existing technologies and data transfer speeds supported by cellular providers.

There are quite many valuable key areas [11] for telecom operators to focus their interest in automotive investments in the following years:

Infotainment & Entertainment:

A sufficient number of telecom operators, for example the American AT&T and Verizon are offering storage services for in-car music and videos. As previously mentioned, Audi in collaboration with Vodafone Telecom was the first to integrate a 4G-capable infotainment system embedded on its commercial vehicles with the launch of the Audi A3 in 2015 [11]. Multimedia entertainment and advanced in-car systems can easily be combined with social network and music streaming applications, creating a new profitability channel for operators around vehicles.

The After Market Opportunity:

On Board Diagnostics (OBD) solutions offer more than in-car wireless connectivity. They offer the ability to transmit data over the cars' Controller Area Network (CAN [11]). That means, any info status generated from a vehicle, can be easily communicated to one or more cloud infrastructures, allowing vehicle parameters processing which could be used for insurance purposes, or for driver or vehicle status. It could, for example, automatically inform the driver over recent events on the road, related to news, like preceding strikes or accidents on the road or even additional remote services, via the RSS radio or Internet feed.

Collaboration between Original Equipment Manufacturers (OEM's) and automotive companies:

Close call mechanical failures or service status will have a massive effect on vehicle maintenance [11]. Data collected from a vehicle's ECU, can be transferred to the car makers via telecom services. This sort of information, if accessed remotely, can help automotive parties remain customer oriented by providing car care solutions or managing repair-services, by organizing the service schedule and updating the car accessories and procurement warehouses. Once, again, Tesla set the market's new rules, as Jeff Evanson, vice-president of the company's Global Investor Relations sector, officially published on February 2017, future selling policies that are planned to include maintenance and insurance costs in the final Tesla's future models prices.

Modern driver licenses and training:

Potential newcomers is possible to be treated with complete mentoring and guidance with electronic equipment and mechanisms, able to track their progress on the streets with statistics and actual facts, rather than just the trainer's perception [11]. Telecom services with geo-tagging systems are capable of monitoring someone's progress and new drivers will be able to comply with driving rules, as police may also have a feedback from the average driver behavior (exported by statistics based on speeding tensions, abnormal car directions and recorded transportation violations), even in real-time. Technologies able to cope with such requirements are SIM, e-SIMs, or OTA services.

Connected wearable cellular devices:

Wearable equipment such as data connected smartwatches or emergency mini-controllers compatible with cellular services may be the next opportunities for telecom vendors to offer emergency support and location services to drivers and passengers [11], in accident incidents or when driving in limited or no network coverage areas.

Telecom Operators that have seized the opportunities first hand:

- ✓ In 2012, Verizon Wireless teamed up with Hughes Telematics on a $612 million contract and today the two companies developed a range of fleet management services for safety, infotainment and efficiency on transportation routes.

- ✓ Deutsche Telekom also shook hands with Daimler in 2013, as a very promising initiative to offer cloud infrastructure, services and connectivity as a complete service provision.

3.1.3. COMPETITION IN THE TELECOM SCENE

The connected vehicles market will erupt as soon as colossal industries like Google, Apple, Samsung and Amazon, grow to become the biggest shareholders of their time. At least, for the moment, telecom companies seem to be the first on the CC pyramid, having the distinct advantage of providing a communications medium which is less expensive than Wi-Fi, available 24/7, with high transmission coverage and seamless operation between switching nodes (cellular base-stations across regions).

Europe’s automotive and telecom industries have formed an alliance to promote automated driving and connected cars. Car brands of high global fame, such as Renault, BMW and Chrysler are all involved in the European Automotive - Telecom Alliance (EATA), as are the local branches of American and Korean manufacturers such as Ford and Hyundai.

Major telecom vendors included in the group are Deutsche Telekom, Telefonica and Vodafone along with telecom and information technology equipment suppliers Ericsson and Nokia. Primary goal of this alliance is to test new technologies for increasing traffic efficiency in smart cities and bring to life automated cars that can sustainably operate in the V2V platform.

The group’s purpose is to design and set the business models required to gear the motorway networks and define the useful technological and financial resources to do that. Moreover, the team will go under great efforts, having to obtain sufficient funding and cooperation from public transportation authorities for their motives.

The telecom-carmaker alliance was set up by Gunther Oettinger, the European Commission’s digital economy commissioner. The European Competitive Telecommunications Association (ECTA), an industry body, is also one of the members of the new alliance. ECTA’s chairman, Gijs Phoelich, announced that the alliance would help connected cars and automated driving come true on a cross-border, multilayered level.

German, globally known carmakers launched a separate alliance called the 5G Automotive Association, along with many of the same telecoms equipment manufacturers involved in the European Automotive-Telecom Alliance.

Again, the aim is to boost development of infrastructures for supporting self-driving cars. However, the membership of the 5G Automotive Association is narrower than the newly-announced alliance as it doesn’t include any telecoms operators and is an industry originated party. The greater alliance will definitely focus on various systems, rather than just the 5G transmission (which is only likely to deploy around 2020) and the new alliance wants to get into testing and simulations this year, but that will only be possible on a limited level. Various formations slowly emerge from different telecom and automotive experts around the globe, giving a promising view of the trending vehicle transformation.

3.2. Telecom Vendors Join Alliance to Car Makers

The freshly announced European Automotive-Telecom Alliance includes six leading sectorial associations, as well as 37 companies [12], telecom operators, vendors, automobile manufacturers and suppliers for both cars and trucks.

The main goal of this Alliance is to promote the wider deployment of connected and automated driving in Europe, methodically. The first move is the advancement of a “Pre-Deployment Project” aimed at testing three major use-case categories:

- Automated driving, which might include high-density platooning, remotely controlled parking, highway auto-pilot and high-definition maps

- Road safety, traffic efficiency and urban optimization for smart cities

- Digitalization of transport and logistics which might include remote sensing and data management

These tests will identify and address both technological and regulatory issues. Among other important elements, the project will seize interoperability issues as well as infrastructure investment to address connectivity needs and the improving of safety and security. At the same time, pilot projects will help to elaborate the basic business models that both sectors can start deploying when investing in these technologies. The research tests are expected to address both technological and regulatory issues.

The project is dedicated to highlight interoperability matters and connectivity infrastructure requirements, based on safety and security for future users. These values will enrich the business models with detailed deployment specifications on the CV technology. In terms of coordination and administration, the Alliance has appointed ERTICO as Project Manager.

So far, the initiative involves the following member states: Belgium, the Netherlands, Luxembourg, France, Germany, Italy, Spain, the United Kingdom, Austria, Slovakia, Hungary and Poland. The Alliance is working towards finalizing the details of the Pre-Deployment Project by December 2016.

3.3. The IoT as a Standard Vehicle Service

Modern vehicles are enriched with numerous sensors and mechanisms, able to prevent mechanic failures, enhance safety specifications and alert the driver on imminent incidents. The sufficient processing power integrated is responsible for the effective management and proper function of all components integrated in the latest cars.

The expanding Internet of Things couldn't but dig into modern vehicles as well. The IoT infrastructure follows a certain topology, where "something" has to be connected and always available to "everything else" as long as all entities follow the same Internet and connectivity protocols. For a successful IoT implementation, most of a car's sensors need to be always connected to the main console, as there needs to be full car status reports and network readiness, either by user request or automatically for the VANET infrastructure.

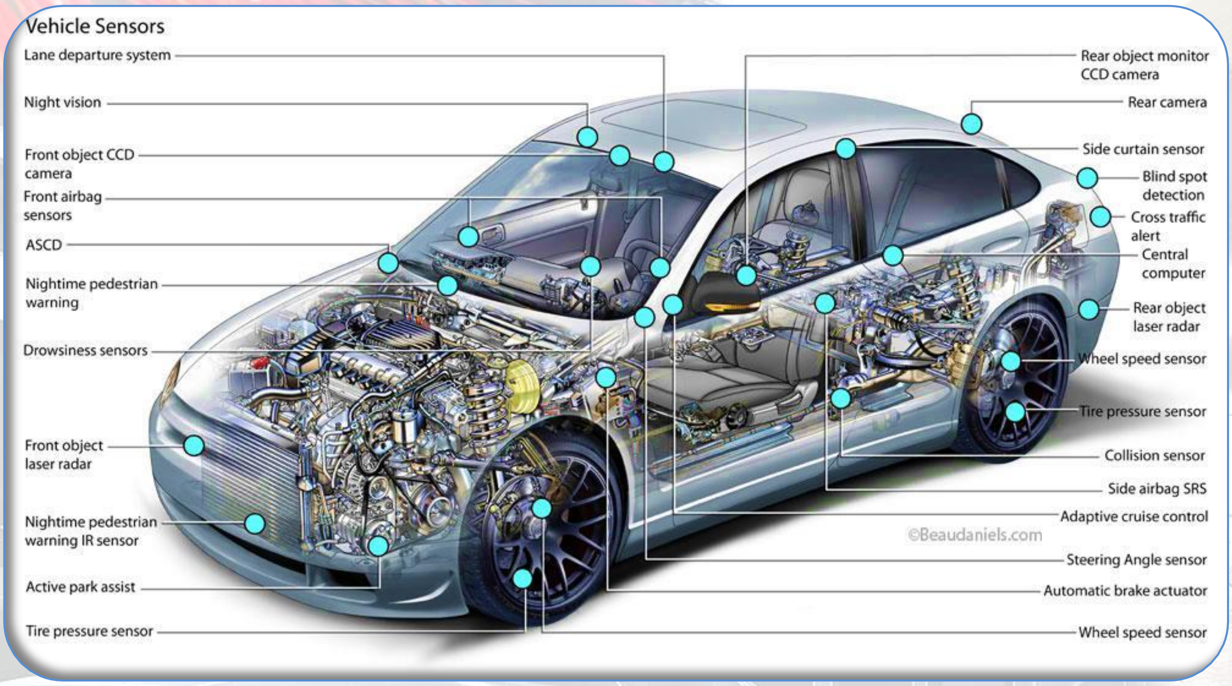


Image 16: *A simple demonstration of only few sensors, installed in different places among modern vehicles (safety, multimedia, electronic assist, car diagnostics etc.)* (beaudaniels-illustration.com, 2015)[25]

The demand for seamless connectivity across cars, motorways and smart devices makes it complicated to synchronize the numerous entities in a widespread network.

There has to be a 100% guaranteed QoS (Quality of Service), available spectrum connectivity and alternative system override rules that will operate when the primary provisional systems fail.

This need is urgently increased, as new driving assistance systems are applied to flagship models, where the driver is even less involved in the end-control of the vehicle. The IoT infrastructure for vehicles was initially conceived as a method of urban traffic management from the European Telecommunications Standard Institute (ETSI).

Although the concept proved to be really ambitious, back in 2008, the network technology and the urban backbone technologies were not sufficient and at the same time, a lot of different systems had to be interoperable across certain areas of interest, but that wasn’t yet manageable enough to work out.

The last few years, researchers and IT engineers brought the concept back to life and have proposed alternative urban schemes that would include full connectivity and services availability with connected vehicles. The only problem here is that the transportation environment should be vastly upgraded with IoT equipment that could manage the new deployment, so that the project could go live sooner than 2020.

Some of the most important telecommunications and IT equipment included availability of Metropolitan Access Networks (MANs), always-on navigation, a wide range of mobile services, Wireless Local Networks (WLANs), smart traffic signs, active safety systems with proactive adaptive cruise control behavior and fleet management, all of which must interact seamlessly without interruptions.

This is one of the most difficult deployments, as it needs to be established and released across many countries simultaneously. The connected car market has to be ready for the future massive customer demand and the products have to be operable and compatible at any moment.

Keeping that in mind, some companies have lately been testing different in-car technologies, preparing the roadmap for connected vehicles. Audi is leading the way, by developing all-around driving assistance, prioritizing the passengers’ safety, with active adoptive components.

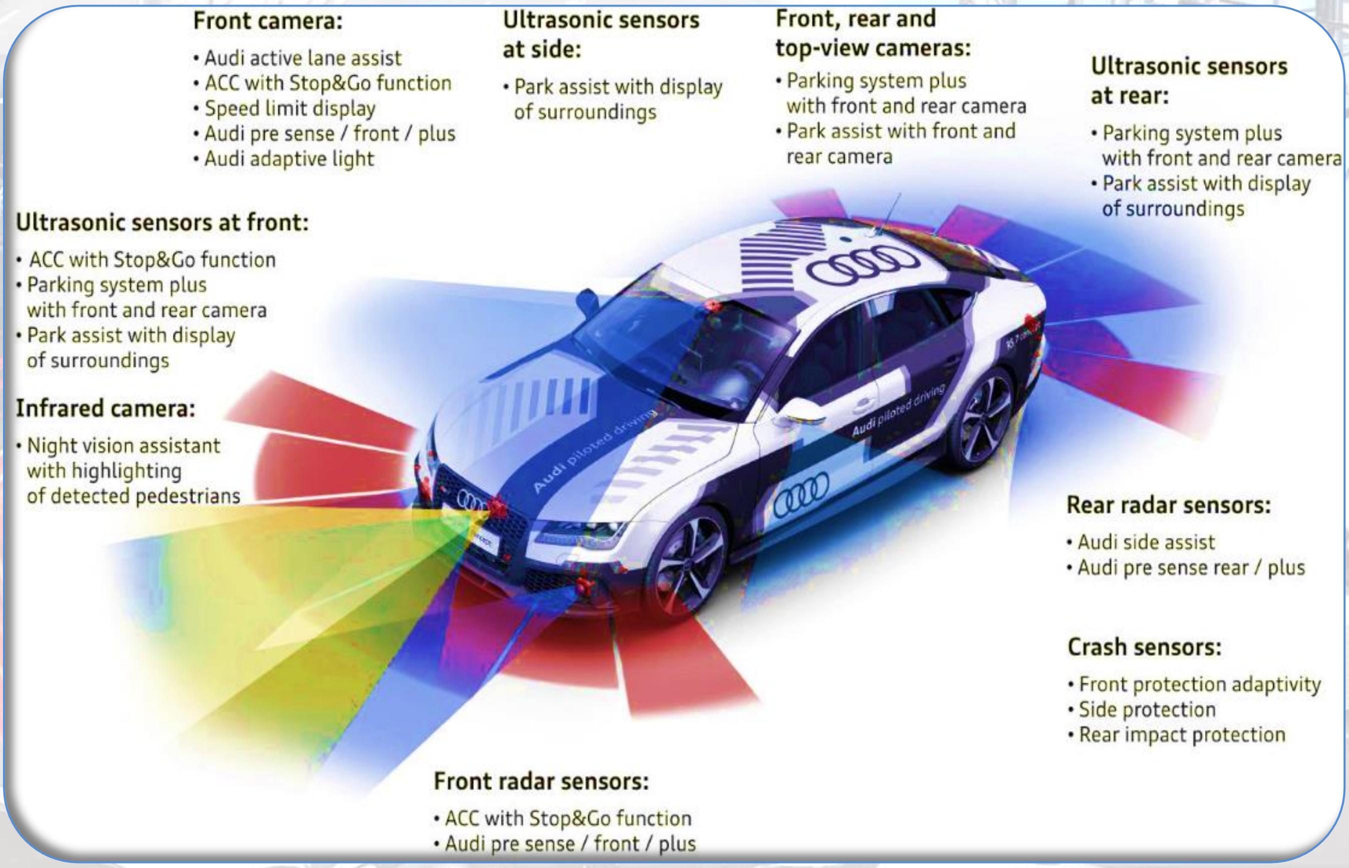


Image 17: *The latest interconnected driving assistance equipment includes route & lane scanner, safety sensors and peripheral impact protection* (thedetroitbureau.com, 2014)[26]

Therefore, car manufacturers have a hard time integrating their vehicles with IoT equipment as standard, without discriminating the essential market needs. One of the main obstacles into this deployment is held upon the inequivalent economic stability between developing and developed states, making the connecter car market's path relatively uncertain.

3.4. Value Added Services on Interconnected Vehicles

The IoT wave brings up many ways of utilizing existing network infrastructures for additional services, instead of just offering a dedicated platform for basic functions. The OTA technology is one of the most responsive ways to update information based on local characteristics or end-user preferences. According to geographic spot, a lot of different services can be promoted and supported, based on route guidance, entertainment, service centers and rest areas across roadways and regional networks.

The multimedia consoles located in certain car models, can be used efficiently with the proper graphical preview, helping the driver fulfil a variety of needs while on the seat.

Smart fuel locator

One of the initial ideas of added services is the gas station locator. The specific service provides the driver with a clear view of where the closest gas station is located, according to the route followed. It calculates the ETA (estimated time of arrival) based on vehicle speed and partial route congestion, as well as fuel efficiency, indicating whether the location is reachable or not. The smart fuel locator was installed on high-end portable navigation systems, as fixed locations which were tagged on the map as hot-spots or points of interest (including restaurants and other).

Although this method was reliable enough, it wasn't as useful in the past, as it seemed. The navigation system couldn't track newer places or facilities, nor was optimized to update the map on removing any invalid places. The software was fixed and each map release was only available for a fee, complicating the user by requiring manual update (by the book). Nowadays, the OTA update of the car console is really user-friendly and easy to update.

The service upgrade is automated, software programmed without human intervention, as long as Internet access is provided. The importance of having an updated map locator leads to fuel economy, time saving and better transportation management along with driver assistance and minimum distraction impact.

Internet access on the go

Another essential service is the web access itself. In a fast pacing environment where people need to be instantly informed, the Internet service is a substantial need that has to be implemented in connected vehicles of any make. The main car display on the front passengers' console can turn into a web access monitor, just like a tablet would. Supplied with haptic feedback and clear, visible tabs, the monitor can operate smoothly as a browser, search engine or multimedia player, able to support multiple audio and video formats, streamed directly from YouTube or Netflix.

This add-on is the ideal entertainment system for multi-purpose family cars or buses that carry many people for distant routes. In the next couple of years, these services will be broadly available to all sorts of transportation means, from trains, buses and even airplanes. By then, telecom vendors will release data plans based on vehicular cellular services on a wide range of scalability and end-user needs.

Marketing & Promotion Campaigns

As car makers get themselves seriously involved in the telecom fields, it is expected for over the top (OTT) players to end up promoting and advertising their products and services with the form of pop-up ads via the cellular connections established. That type of advertising is believed to be a great opportunity to commercial and wholesale products and services, as long as they comply with the certain market and user policies, upfront.

Ads will be available as either scrolling highlighted text banners or as small audiovisual representations on a limited part of the vehicle's main dashboard. The show time period of ads will also need to be calibrated accordingly, by the vehicle state and the driver's preferences. This way, once again, no distractions shall interrupt the driver while on the seat. In addition to that, a new marketing method of promoting goods will overcome the outdated radio ads.

Online Service Calendar

With the technology convergence, car makers will take the opportunity to keep their customers even closer to them, by leaving no option of choosing unauthorized service kiosks for their vehicle maintenance. The main concept behind this function is to ensure, as long as vehicles will get more and more tech-loaded, unofficial or uncertified resellers and engineers will get pulled out of the league.

Each vehicle will have the intelligence to decide when the next service will be scheduled and who will do it (the authorized service centers). This equation will increase the automotive and telecom income and customers will have to agree to that, by reading and accepting the end-user terms before buying one of these intelligent vehicles. The concept also includes automated payment methods based on user valid credentials, either by NFC tagging, by smartphone pairing or cellular joined credit balances.

Emergency Callback (advanced e-Call)

In cases of accidents, modern vehicles have to be prepared for the "worst scenario". All those multiple sensors spread around each vehicle, need to be capable of identifying the damage level of the surrounding frame and then "decide" whether the authorities and emergency lines should be alarmed, about the location and the damage, as well as vital signs of passengers. The OnStar platform is based on this architecture, but only partially.

Future vehicles are expected to do many more actions than just call the 112 line. Some of the later technologies are believed to include interactive first aid guidance in case a passenger faces a seizure or stroke, by properly offering instructions to the rest in the cabin. It is also possible that vehicles in a local area can share their location directly with the nearest hospital on the local VANET cell at any moment, a feature very useful for unexpected premature pregnancies or other injuries occurred out of the vehicle.

CC Service Level Agreements

Small businesses and large corporations cannot be excluded from the profit of both parties, as explicit services are always a businessman's attractive tool, provided it can simplify the whole procedure and maximize the company's performance. Service Level Agreements have been around the telecom environment for quite many years, as they refer to large corporate schemes by providing guaranteed services of telephony and xDSL connections for business stability and maximum profitability.

The connected car could as well utilize cellular – vehicular data and voice contracts for VIP customers and / or demanding individuals or businessmen that need uninterrupted service or assistance, while on the go. Late conference arrivals could be eliminated by offering data and connectivity, sufficient enough to execute a video conference while stuck in traffic.

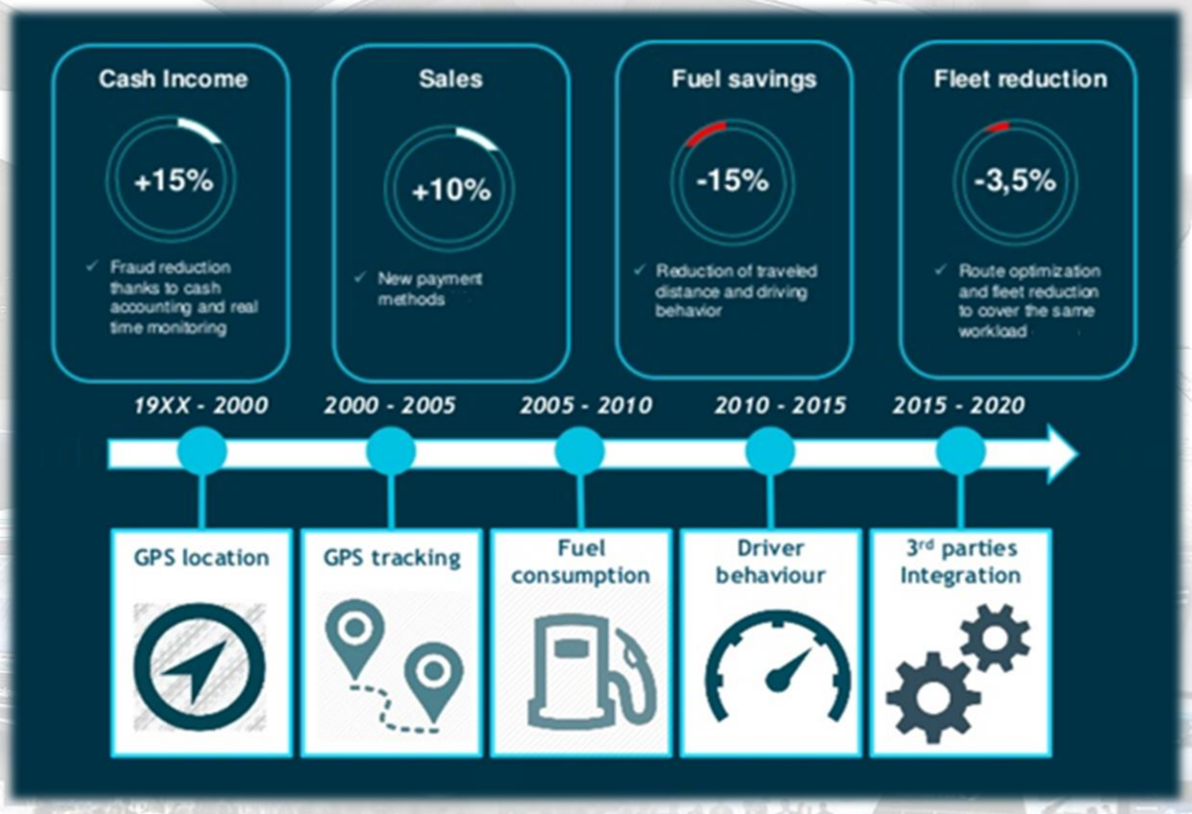
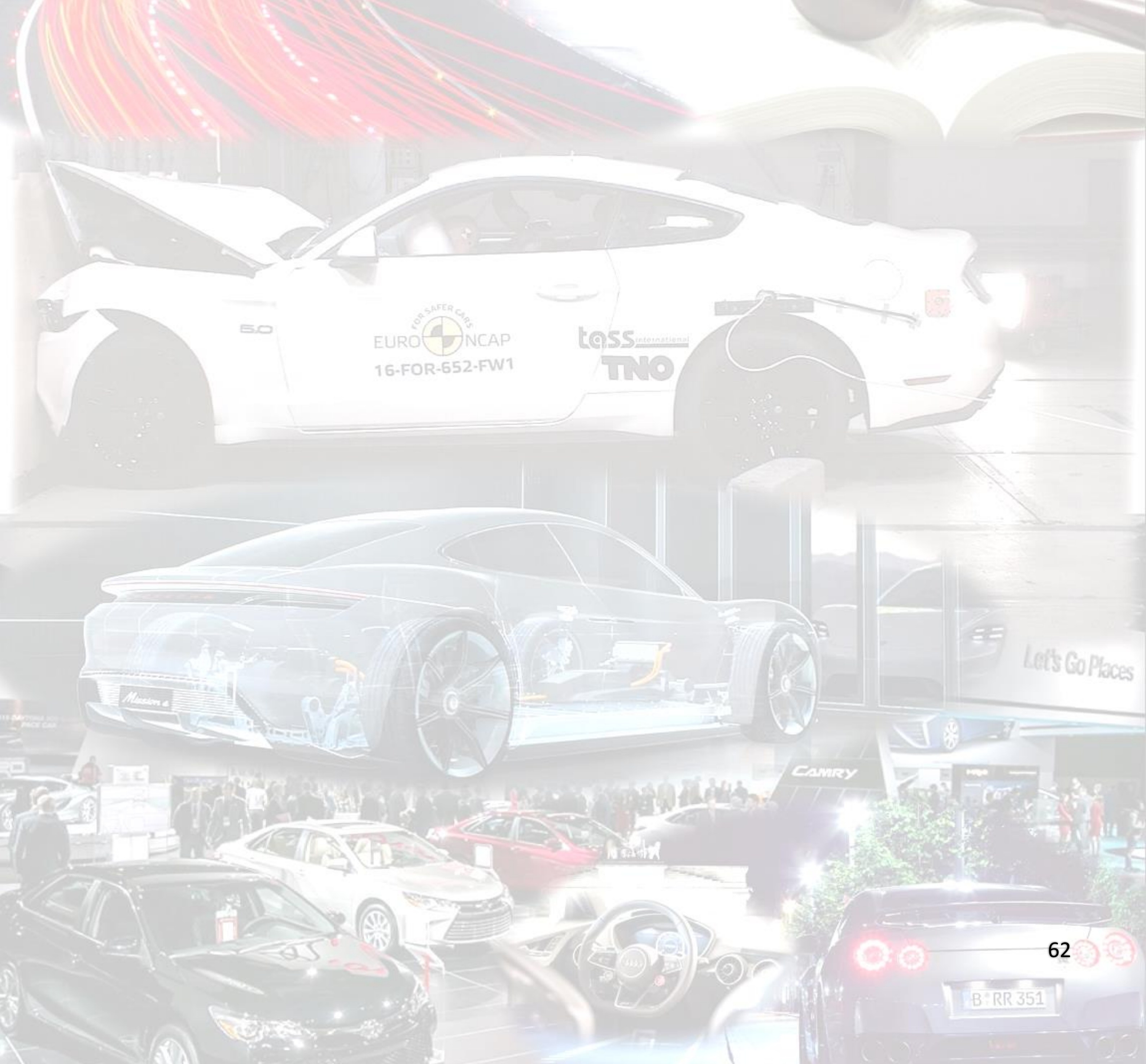


Figure 2: *A presentation highlight from Telefonica, issuing the action points and key advantages that can emerge from utilizing value added services in the modern industry (Telefonica, 2015)* [27]

The Cisco WebEx live conference platform is a great example, currently supported only on laptops, tablets and smartphones.

Another promising service, soon to be established, is a full cargo tracking service on a truck fleet route between neighbor countries. Similar services would form ideal SLA combinations for transportation agencies. Apart from that, the equivalent fee of SLA services is estimated to attract many users and enhance the profitability by offering upgraded and secure services applied on connected vehicles. Skype also joined the car industry by integrating conference and calling services in Volvo cars, as a Microsoft - Volvo duo. For the record, they initially supported voice only dialing via the CC connection, as a purpose to ensure safety and minimize distractions, while driving.



Chapter 4th

Boundaries of Connected Cars

4.1. Data Sensitivity over In-car Technologies

Privacy-related issues are of high critical impact, concerning wide diffusion of Vehicular Communications (VC). Many threats tend to affect multiple data transfer procedures, supported by malevolent remote users or malware coded scripts. After the 2000 virus, it was already widespread that any electronic equipment could be "poisoned" by Trojan viruses and hacking attacks at some point, leaving no more thoughts to those who are opposed to involve themselves to any technology in their daily routines.

The latest smartphones are equipped with too many separate communication protocols and support a variety of file formats, plus with oversupplied memory capacity in them, they can record or store anything no matter the required flash memory.

Cellular connections are by far considered to be the safest ones, as there is no physical network topology neither the potential a cyber-attacker to be aware of each user's online status or cell location. Instead of using vulnerable untrusted Wi-Fi networks, 3G, LTE & 4G networks use full end-to-end encryption, if the sender devices are data-encryption powerful as well.

The mobility needed in the connecter car environment, requires insane response times, a large available signaling bandwidth, enforced privacy, security coverage and guaranteed data encryption. The method and topology that is about to be issued in the automotive industry applies the same way it does with smartphones. Connected cars are just going to operate as "bigger" smartphones on four wheels.

The doubt about data sensitivity that's been deeply expressed by so many people around the globe, is the key factor to identify whether or not the connected vehicles will have a certain marketing penetration or not. Other significant question marks are stated later in this chapter, as end-users are predicted to seek deep knowledge over everything that deals with the mobile data management confrontation by the telecom vendor they will select.

The main concern focuses on specific yet sensitive parameters that have to be handled with extended confidentiality, naming few of them below:

- Current vehicle & user location
- User preferences, based on cookies and web browsing history
- Sensitive and/or private data, based on vehicle routes
- Car cabin status (potential unauthorized real-time interception of private conversations, threatening eavesdropping attacks etc.)
- Vehicle protection from remote control violation (unauthorized vehicle control override exposure)

A considerable EU-based 'Connected Car & Data' survey

FIA (Federation Internationale De L'Automobile), recently commissioned a public survey in 12 EU countries, as a purpose to analyze and log the consumer attitudes over the approaching connected cars trend. The actual transmitted data the connected cars generate are 100% personal sensitive info, tunneled all the way to the World Wide Web and the survey made sure this would be communicated on all participants.

The first part recorded the familiarity of drivers with the connected car -environment. In some countries, like the Netherlands, the majority of the respondents, had least to none awareness over the connected vehicle philosophy and were not even interested in that kind of transportation pattern.

Other countries, such as Germany and France were found to have great awareness over the connected cars platform, being able to categorize the basic requirements such an implementation consists of. The very first conclusion of this survey was that there was a significant variation across EU countries, over the specific car-data pattern. This indication could only show how difficult it will be to equally and accurately establish the connected car market on similar countries with common transportation frameworks.

As the survey continued [13], all familiar respondents expressed their point of view over reasons that would lead them to trust a connected vehicle against a conventional one. The three most important reasons were:

- Increased safety
- Optimal fuel efficiency
- Effective congestion avoidance

The market sample was later split in six basic shares, with the biggest of them being those who were actually interested in connected vehicles but on a second thought were hesitating to buy one (25% of the total sample). Those who were comfortable and positive on connected cars (20%), were equally interested in in-car entertainment systems and car-related features, as they were more confident than the rest of the surveyed sample over the data safety around vehicles.

The distant ones (19%) would only partially accept to have their personal data transmitted and shared for basic functions such as remote diagnostics or fuel consumption reduction. The part of the sample that was rather anxious and not interested (14%), were participants that felt unprepared to share their data as they were very concerned about data security. They would even read the entire policy, highlighting their rights before buying a connected vehicle.

Finally, the rest sample (10%) expressed those who were against the connected car deployment, either due to little awareness over car & data functionality, or because of a lower than basic academic level / education. They weren't able to accept the dominance of this platform, as they would never seek to buy a car with an integrated connectivity. The human interaction with connected vehicles had to be measured and evaluated, in order to identify the reasons and conditions under which drivers would select to trust connectivity mechanisms [13] inside their cars.

The next figure depicts a detailed image of the comfort the surveyed respondents had, by sharing any vehicle data:

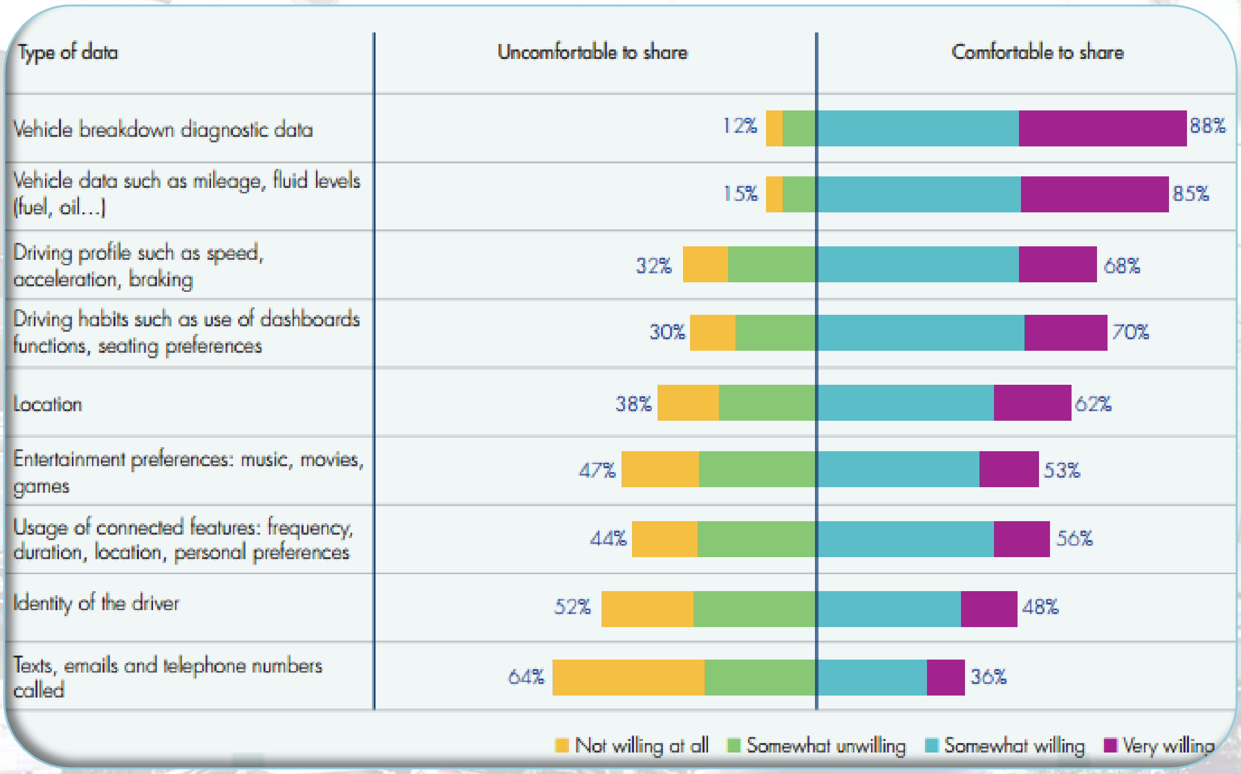
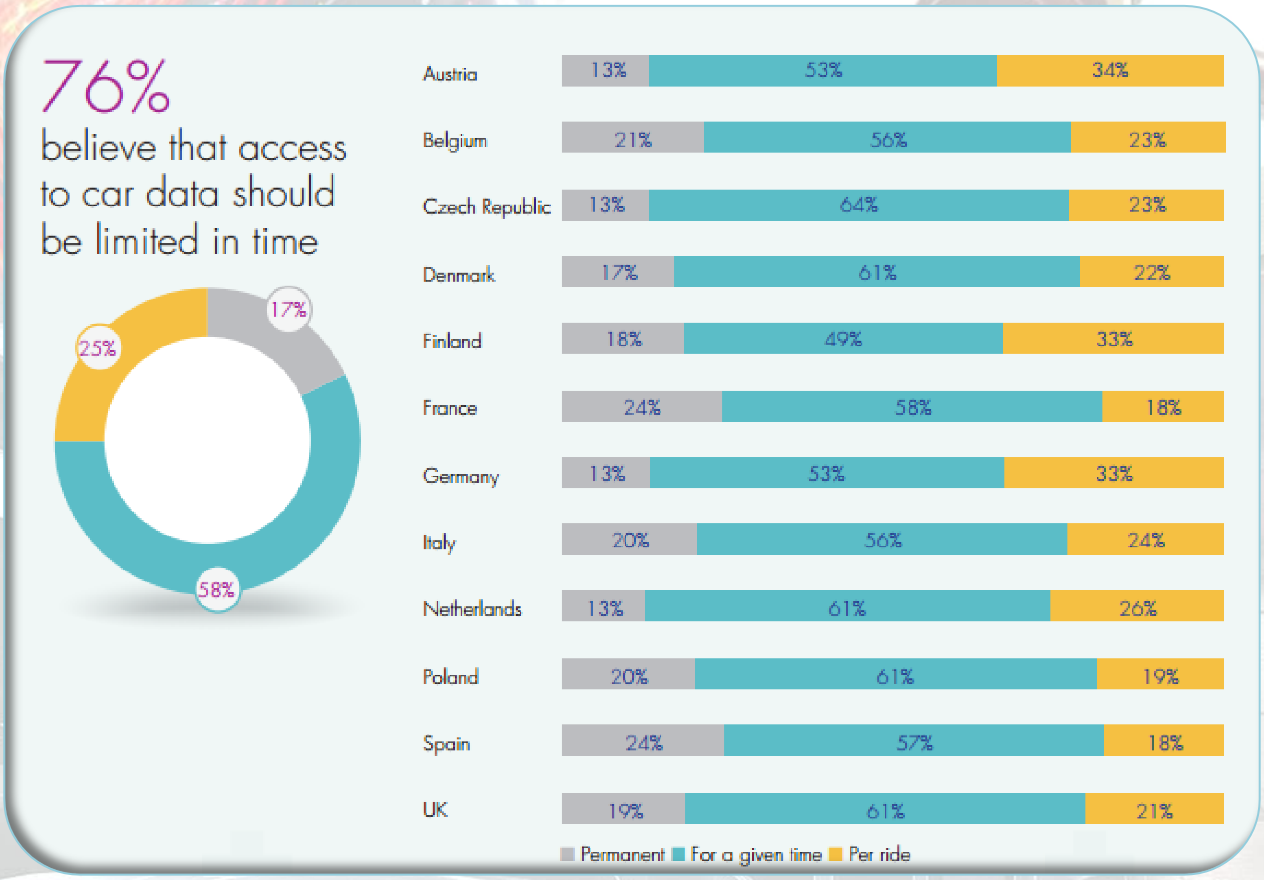


Table 5: *The FIA data sharing preference ratio (user preferences) over connected vehicles* (FIA, 2016) [28]

Another very important detail that forecasts obstacles in the connected car dominance was that many of the distant respondents indicated limited willingness to pay for any car connectivity features. For instance, only 33 percent of all respondents stated they would pay an additional €100 fee (approximately) for smartphone and data integration and just over 20 percent would ever be willing to pay for subscription-based connectivity services, accompanied with a new car purchase [13].

Other than that, the participants of every surveyed EU country were questioned over the appropriate duration a connected car should actually be on an on-line state, if not always:



Graph 5: ***The participants' opinions over the connectivity duration of data-connected vehicles, based on each of the EU countries involved*** (FIA, 2016) [29]

The concerns about data sharing while on the driving seat aroused a lot of inquiries that have to be cautiously taken into deep consideration. The connected car is a new trend and a great part of the EU population seems to not having accepted the car market alteration that will follow in the future. The only thing agreed on all sides, was that consumers want legislation to protect any user-data (either European or International) [13]. The need to secure user-generated data, defines the urgency to develop a specific legal framework to protect consumers' rights at all costs.

4.2. Security as a Crucial Factor

The early technology upgraded vehicles brought up various assistance tools and extra comfort, by supporting many functions of the vehicles, requiring only minimum effort from the human factor. Hydraulic systems, additional ride-by-wire support, parking assistance and electronic braking systems (EBS) were all installed in modern vehicles as to ease the user and at the same time, offer guaranteed safety specifications on the road. As with computing systems, the car scheme couldn't but get under certain threats, in a rather exposed way, by unauthorized remote factors.

Time to talk about cyber hacking. In the last almost two decades, many separate cases were reported among Internet users, who found themselves in deception, originated by remote hackers. Ever since those reports increased in number, professionals of specialized computing systems science fields were hired by OS and applications providers, in order to find any vulnerabilities or security gaps in their systems, whenever they were operated while connected to the World Wide Web. Many cases included piracy, personal and banking data theft and even stealth real-time conversation tracking.

During the technology convergence, vehicles steadily turned into mobile computing sets, able to process data and control different car parts. This, lured malevolent users into attacking vehicles, serving purposes such as gaining remote control or even grant access to specific functionalities, like braking and engine deactivating commands. The latest connected vehicle actions taken into deep consideration by stakeholders, brought about a great concern over security escalation and assurance matters, significant for the forthcoming vehicle diversification.

4.2.1. Reported Threats of Vehicle Hacking Attacks

Connected cars can contain more than 50 different electronic control units connected through the controller area network (CAN) or other networks. Those ECUs communicate with each other and operate through the CAN bus, broadcasting digital messages called CAN packets. If those packets are not authenticated or highly encrypted, vehicles may be prone to remote hacking through the integrated wireless or cellular modules. The vehicle's wireless technology may also enable unauthorized access to other systems and data collected by the vehicle, such as location data and potentially payment card data used for dashboard shopping.

In 2015, two professional security analysts, Charlie Miller & Chris Valasek tested a few strong hacking scenarios, in cooperation with Jeep, the famous 4x4 company [14]. The purpose of this effort was to prove how someone could interfere to the direction system of a Jeep Cherokee model, in addition to how effective the hacking actions would prove to be, if executed methodically and with full effort. Although the specific SUV was only connected to the Internet via its main entertainment console, the two analysts managed to hack the vehicle, infiltrate into the steering system and eventually drive the vehicle off road, from a ten miles distance.

At that time, it proved useless for the driver to switch-off the engine or try to handbrake the car, as it wasn't responding to any actions. The driver also expressed his concern over the capabilities of hackers with internet access, as not only did he lose control over the vehicle, but the ventilation system started pouring cold air in the cabin, the dashboard had all needles maxed out and the radio kept switching stations so fast, that the fear of being trapped inside a 70mph vehicle, was one of the strongest ever experienced. And if that was only a "safe" and tested scenario, imagine what it would be like to happen in someone's actual life. The analysts also stated that cyber-attacks of this kind could easily happen from across the country with extreme accuracy, if they are executed under a high-speed data connection.

Image 18: ***Actual footage of the remotely hacked Jeep Cherokee, including a trapped driver, locked doors, a failed braking system and the total loss of steering control*** *(wired.com, 2015)* [30]

Conventional and legacy cars are easily exposed to life threatening hack attacks, once connected to the Internet. The actual location of a vehicle could provide carjackers the ideal attack plan, especially for VIP targets, like politicians, or law and police forces.

On June 30 2016, another hacking scenario came to publicity, this time on behalf of Tesla's auto piloted vehicles. Elon Musk hired many security researchers in order to detect vulnerabilities and gaps on the interconnected platform of the high-end vehicles.

A team of Chinese security researchers, members of the Keen Security Lab group [15], found out a breach, which offered them the ability to hack the car's controlled area network (CAN bus) and eventually take control of everything the vehicle was equipped with. The hacking gap was existent on two Tesla models, S P85 and 75D, but the group implied it was possible to hack other cars with the same method, as well.

The described above attack, required the car to operate under a malicious Wi-Fi hotspot (set up by the hacking team) and this could only be triggered when the car's web browser was used. Now that cars such as Tesla's are increasingly high-tech and connected to the internet, cybersecurity has become as big an issue as traditional safety features.

Finally, it is clearly stated from cyber security researchers that there are more than 470.000 modern vehicles [15] currently on the streets that can be easily hacked, if connected to the Internet. So the threat is out there somewhere and today's cars are not armed with any basic level security firewalls.

The connected car philosophy sets its axis above safety and security, so it is crucial to define the next steps towards effective cryptography and signaling security methods for a reliable and promising V2I & V2V environment in the future.

4.2.2. THE VIPER PROTOCOL

A major threat to privacy in VCs is the traffic data analysis. Considering this as a fact, some important researchers came up with a very reliable V2I communication protocol. VIPER, also known as Vehicle-to-Infrastructure Communication Privacy Enforcement Protocol [16]**,** is inspired to solutions provided for the Internet and cryptography universal re-encryption in general. The base of this protocol is to have vehicles not to broadcast their data directly to a local RSU, but to have all vehicles acting as aggregation access points with OBUs (On Board Units).

Figure 3: *Demonstration of V2I and V2V communication combinations, including ready-connected urban infrastructures (RSUs) and vehicles that operate as repeaters (with OBUs) broadcasting the useful information towards close passing 'mates' on certain location ranges* (analysis.tu-auto.com, 2015)[31]

Messages are encrypted with a public key crypto-system that allows re-encryption of messages. Both telecom vendors and car manufacturers are progressively paying more and more attention to Vehicular Communications (VC), allowing vehicles to connect to each other and with the roadside infrastructure, as to form a secure and performant VANET eco-system.

The mix consists of nodes belonging to the same group, where a group is defined as the set of vehicles registered within an RSU. Combining these techniques in an original way, leads the protocol to be strong against traffic analysis interruptions while preserving its scalability.

The protocol's analytical results suggest that it also performs well among key performance indicators like queue occupancy, message path length and message delivery time. Simulation results show that the overhead introduced by VIPER in terms of extra bits required, computations, time delay and message overhead is feasible even for increasing requirements on the security of the situated cryptographic mechanisms.

RSUs are placed along the roadside and are controlled by a network operator [16]. VCs will enable the development of systems to support several services, for instance road safety, traffic information diffusion, automatic tolling and entertainment. The expected development of VANETs will involve millions of vehicles worldwide, making that network the most extended form of mobile ad-hoc networks.

However, the nature of the wireless communications makes eavesdropping particularly easy. A potential remote attacker needs to do few only actions, like disperse “hacked” IoT devices across the target area of the network that it wishes to monitor. In addition, a mobile adversary could consequentially follow a target vehicle while being outside the line of sight, simply by packet “sniffing” the messages, sent by the target.

At the same time, safety messages provide even richer information on their sender. This essentially allows automatic tracking of the vehicle, which eventually reveals private information regarding the activities of the driver. The wide availability of VC-compatible radios (802.11-based) makes such a threat even more credible.

Furthermore, VANETs introduce a number of challenges to the research community like high node mobility, nodes variation and several security issues [16]. For instance, exchanged messages can take part in road safety applications therefore, it is fundamental to take security into account when designing protocols and mechanisms for VANETs. In particular, security requirements include authentication, data consistency and integrity, availability and privacy. In the Vehicle to Infrastructure Privacy Enforcement Protocol, the focus is based on non-time-constrained communications that are usually involved in applications like automatic tolling, traffic information diffusion and entertainment.

4.3. Data Privacy & Law Enforcement

The organizations involved in vehicle-to-vehicle & vehicle-to-infrastructure communications, are specialized in different fields of expertise, therefore all of their embedded services have to be consolidated and monitored in a specific way, as to avoid any beneficial conflicts between telecom vendors, automotive groups and transportation departments.

The IoT is daily characterized by heterogeneous technologies, which lead to the provisioning of innovative services in various applications. But the greatest and most important role is the assurance of security and privacy requirements.

These include data confidentiality and authentication, access control within the IoT network, privacy and trust among users and the enforcement of security and privacy policies on all private and public network infrastructures. Up to this day, due to different standards and communication stacks involved, it is extremely complicated to set such compatible and safe CV platforms. Furthermore, the increasing number of interconnected devices provokes scalability issues and security matters.

Among all CV infrastructures, these are the greatest IoT challenges [17]:

i) Authentication
ii) Access Control
iii) Privacy
iv) Policy Enforcement
v) Trust
vi) Mobile Security
vii) Secure Middleware
viii) Confidentiality

Access control, deals with numerous users, separately treated by **authenticating** dedicated credentials or very strong certificates, just like it works in cloud and e-mail accounts. The access control must be security developed and allow authorization strictly to users who have acquired user rights identical to the access type.

Privacy refers to individual data protection. The databases, under which privacy rules are applied, are responsible for the personal information accessed by administrators. Privacy policies are applied on data streams generated by the end-users who own digital devices able to export data flows. It is user-defined what information can or should be accessed by the database management systems. The system administrators that provide these systems are always informing end-users about the existing privacy policies applied, by requesting agreement to the published terms.

Policy enforcement describes the rules, used to force a group of strict actions in a system. These rules are significant for ensuring order, security and continuity on data recorded on these systems. Through technology evolution and with the software defined networks the rules are becoming more accurate and with great scalability.

A subjective model for the management of **trustworthiness** is defined, which builds upon the solutions proposed for Peer-to-peer (P2P) networks such as two entities (two or more cars). Each node (local CV network) computes the trustworthiness [17] of its nearby vehicles on the basis of its own "experience" and on the "opinion" of the common -passing by- "mates". As a consequence, a node chooses the provider of the service it needs, on the basis of this highest computed trustworthiness level.

Devices and systems that are moved from one network infrastructure to another must be equipped with protocols that apply the same way across all functional nodes they may operate on. In terms of **mobile security,** cryptography, instant authentication and privacy protection are basic values that should prevail in an authorized connection in the IoT environment and especially in the connected cars scheme.

In order to sustain a successful IoT integration and functional communication technologies, a **secure middleware** is required, able to cope with the defined data constrains and the transition from one communication technology to another, in a compatible platform across different operating systems.

Confidentiality comes close to data anonymity and integrity, as those attributes need to be ensured and guaranteed among with authentication and authorization mechanisms in order to prevent potential system violations (security threats by humans and / or devices) from gaining unauthorized access.

The need for neutral and comprehensive mobile network coverage to strengthen the connections between data devices brings telecom companies in a new investment strategy, where mobile infrastructure and tele-informatics are in prime position.

Based upon these fundamental values, modern outsourcing companies, such as Baker & McKenzie come to fill the greater image, proposing alternative duty assignments on multi-level projects, through which connected vehicles should be sustained and operational. Different aspects of the connected car can prove to be distinct case studies that could possible enlarge into greater separate divisions (including promotion, intellectual property, consumer protection, industry regulation, liability etc.).

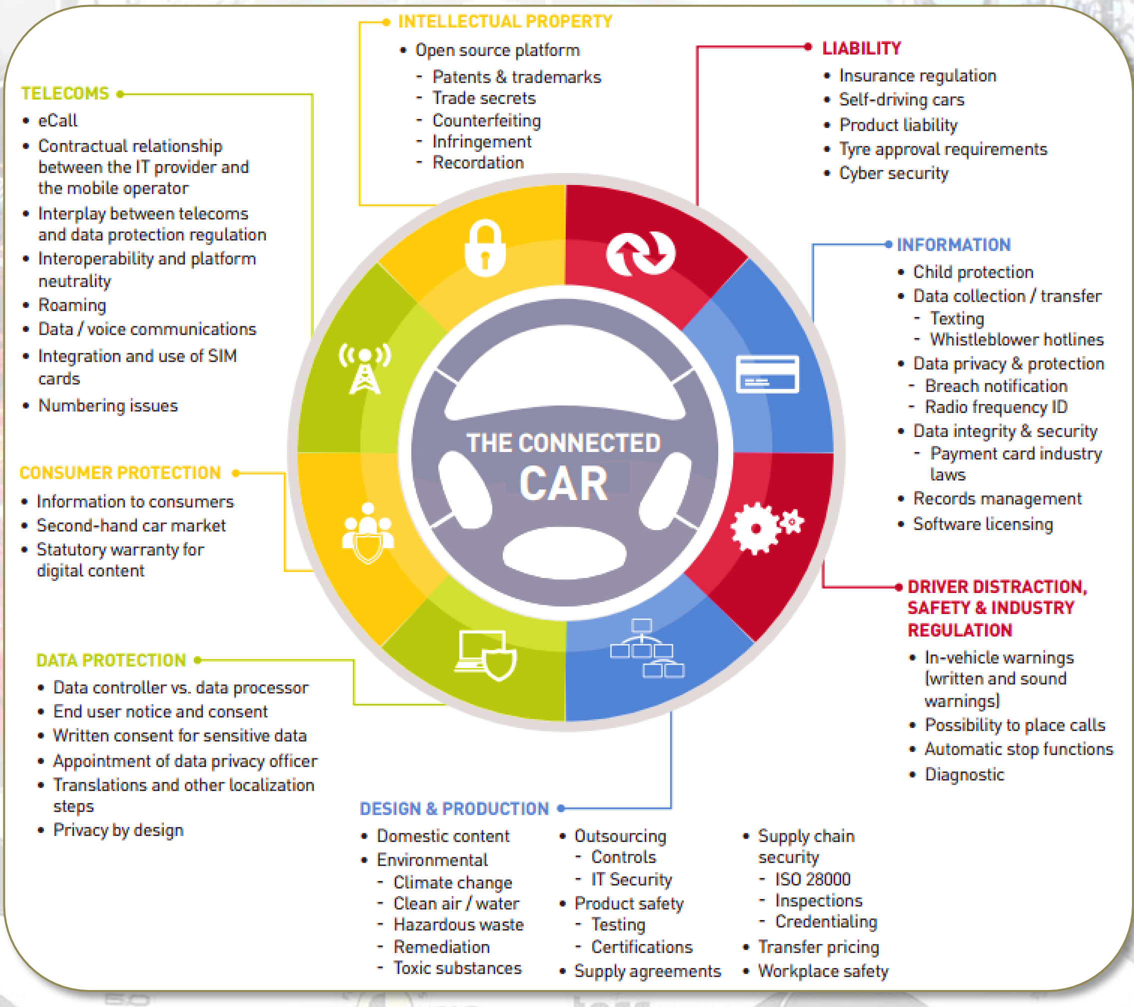


Figure 4: *The Baker & McKenzie connected car map, including almost all law and digital segmentations, a CV platform consists of (Baker & McKenzie, 2015)*[32]

4.4. Safety-related Issues

Keeping in mind the multi-dimensional character of a CV, by the moment someone chooses to board in a connected vehicle and until the very end of the journey, there has to be an unambiguous consent of any procedure or application that is installed and allowed by the end user(s) (driver and / or passenger(s)). This can be easily explained, once the connected vehicle ambient is expected to operate as a smartphone. Smartphones, according to global manufacturing standards, provide certain software and application support, which can be variously escalated by user-only allowance.

For instance, the access needed by Google Maps on the embedded GPS location services, is strictly activated by user interference and never by the application's software (at least not initially). Before any scheduled trip, data shared between any public vehicle-driver-location schemes, have to be equally consent by the end user(s), while at the same time, the application server has to treat any data exchange and storage procedures by the regulations set in the user agreement manual.

Consequently, any onboard incidents that may occur tend to trigger data that can only be transmitted in an encrypted, secured and confidential way. On any other circumstance, the end user agreement or any user-requests are violated, which means that private information has been exposed without consent, something also known as a structural violation or security breach.

The problem with transmitted data over a vehicle network is also translated into safety gaps, if mistreated. Different aspects of a double collision accident, can lead to false accusations or conclusions over who of the involved drivers is the liable one, if no mechanic failure is logged during the incident.

Apart from the in-car activity, there are also lots unavoidable cases where intelligent systems completely fail, due to manufacturing vulnerabilities or software versions with in-code bugs. Whichever the scenario, both automotive makers and telecom vendors, are obliged to equip all cellular or OTA data-supported vehicles with proper and precise adaptive systems including expanded user-log recording of the whole journey. This way, any multiple collision incidents will be easily distinguished and weighted accordingly, by comparing driving behavioral actions between involved vehicles, recorded at the exact system time.

The supervised driver-logs method is expected to minimize accidents' cases consummation duration and significantly support the local authorities and stakeholders (police departments, post-accident driving assistance and insurance companies), altogether.

More in advance, the C-ITS group ordered an action point to emphasize the urgency to revise the European Statement of Principles on Human Machine Interface [6] (ESoP on HMI) because its content needed to be adapted to the current platform development into new vehicles, as a formal EU Commission recommendation. Relevant existing standards need to be evaluated before they are implemented. Many standards were developed prior to C-ITS and may not fulfil all the requirements needed for a successful and sustainable implementation, especially in hybrid systems.

The multiple presence of various vehicles on the road among those equipped with the new C-ITS, may create some safety challenges. While the EU Transportation regulations tend to increase the CO_2 emission taxes annually, not many vehicle withdrawal policies are applied at the same ratio. The major safety risks expected to show up, refer to all those vehicles that have limited or even no connectivity compatibility with the C-ITS platform, making the vehicular network practically unstable and inefficient.

So far, the options and possibilities for successful C-ITS technologies are significantly limited. The variation between vehicles with or without relative equipment through the deployment is what makes it particularly complicated to establish the needed infrastructures. Some of the strongest recommendations that have until today been agreed upon, are listed below [6]:

- ✓ Execute further researches between "connected" users and legacy vehicle drivers.
- ✓ Enable further driving training sessions, for newcomers and current CV users, purposed to present rules and techniques around connected driving, with hints and tips on system capabilities and limits, plus awareness over manual driving errors or attention distraction.
- ✓ Enact traffic rules and further automated functions during the C-ITS deployment that will ease the sponsors while installing the driver assistance systems.
- ✓ Promote the important safety information and driving behavior between equipped and non-equipped users, as a measure to increase transportation awareness during the C-ITS deployment.
- ✓ Facilitate C-ITS simulation sessions for the users that are not yet equipped, by using real-life scenarios of connected vehicles that exchange information with the urban infrastructures or with other cars (V2V & V2I data exchange).

The recommendations seem quite ambitious and hopefully the connected environment will go deep into legacy users' minds, as an alternated, developed lifestyle.

Awareness & Training

The European Commission agreed that many road users, including drivers, will not be adequately aware of the functionalities, safety benefits and limitations of the new technologies for a certain period, around C-ITS. The group also insisted to incorporate official campaigns on driver training schools, either on a pre- or a post-licensing level.

The additional suggestions aimed at avoiding road safety risks, resulting from the lack of awareness of some road users concerning C-ITS and other driver assistance technologies [6]:

- Informing road users about the existence, functionalities and limitations of the new technologies (e.g.: raise public awareness through actions taken by relevant stakeholders, like insurance companies and rating organizations such as the Euro NCAP).

- Adapt driving license education to inform about the technologies that new drivers are likely to be confronted with, in particular safety-related ones, but also others, such as traffic management, automated route guidance and eco-driving.

- Encourage pre- and post-license training trial exhibitions, hopefully linked to the purchase of a connected vehicle (new or used), to update drivers concerning the new safety-related technologies and to increase connectivity management experience.

- Encourage vehicle manufacturers to offer complete briefing information on the new technologies fitted through sales agents or official car centers, including a possible pre-order demonstration of the connectivity capabilities as part of the sales package.

4.5. End-user Rights

The developing vehicle-telecom blend will get tunneled through certain distribution pre-sales channels, where the interested market share, will unavoidably be obliged to go through an end user license agreement of the final product. For a buyer to obtain the car that fits the most, every single aspect of the product must be clearly reported and delivered, officially naming the user rights, prohibitions and warnings, next to the operational compliance, according to manufacturing standards before final delivery.

Application and OS developers are also informed over the distribution policy that exists before embedding their services into certain electronic markets such as Android or iOS App Store & Microsoft market.

Similar license agreements [18] are applied among many modern platforms and services of the same field. Especially now, where the two major mobile OS players (Google & Apple) have integrated many apps in single back-bone infrastructures, the compatibility and scalability of the current tech solutions, lead the way to the connected vehicle scheme.

The early predecessors, Android Auto and Apple Car Play, transformed the vehicle's main HUD into a smart center, by utilizing Bluetooth connection and screen mirroring, in order to offer ease and user experience improvement while on the go.

Image 19: *Apple CarPlay™ & Android Auto™ in action* (androidpolice.com, 2014)[33]

In the connected cars environment, the extended usage of technology and applications will inevitably handle numerous of legal sanctions, a point from where various stakeholders will defend their position over connectivity matters and sensitive information in between their vehicular environment.

The end user license agreement is certainly expected to include application & telecom fields of utilization, as a standard product-buyer protection mechanism. As in currently available applications and telecom service contracts, some of the substantial legal categories to be contained, are:

- ✓ Scope of License
- ✓ Consent to Use of Data
- ✓ Termination
- ✓ Services & 3rd Party Materials

4.5.1. Scope of License

This category is correlated to the allowance of use of any licensed (official) applications, provided by the respective application providers. Strong restrictions are stated, like no compatibility on any other platforms or systems that do not follow the official requirements as registered and validated on certain sections of the respective Application Store Terms and Conditions ("Usage Rules") [18]. It is embedded as a ruling order over what privileges and restrictions the user has over released applications or services according to compliance and valid user policies.

All scopes of licenses must clearly state that the products or applications are being excluded from any rental, leasing, lending, selling, redistributing or sublicensing actions, as they are only purposed for personal use, under the Licensed Application.

Further user restrictions applied by the scope, are material copying, de-compilation, reverse-engineering, disassembly or any source-code modification of applications. Also, any updated terms are only released by the application providers solely.

4.5.2. Consent to Use of Data

On this section, the application providers inform users about the technical data and the related information they periodically may collect, exclusively for product improvement and research actions.

The statements on the 'Use of Data' include device, system and application software data, as well as peripherals information and diagnostic logs that are collected and utilized for development and user experience purposes, plus to properly provide seamless services over legacy or outdated systems among newer ones [18].

All of the collected info is not impersonal and cannot be manipulated to identify physical identification or personal behavior, as it is purely technically originated and oriented.

4.5.3. Termination

Termination determines the end of a service agreement, either if finalized by the application provider [18], or by the end user. The statement also includes imminent termination of agreement, if any of the two sides, does not comply with the terms of the license.

4.5.4. Services & 3rd Party Materials

The Licensed Application states that enabled access to application provider's and 3rd party services (collectively and individually, "Services") may occasionally occur, as any use of these services may or will require Internet access, where the user accepts additional terms of service by that.

Other notifications and statements include:

- Certain services may display, include or make available content, data, information, applications or materials from 3rd parties (3rd Party Materials) [18] or provide links to certain 3rd party web sites.

- By using the services, the user acknowledges and agrees that the application provider is not responsible for examining or evaluating the content, accuracy, completeness, timeliness, validity, copyright compliance, legality, decency, quality or any other aspect of such 3rd party materials, web sites or services.

- The application provider does not warrant or endorse and does not assume and will not have any liability or responsibility to the user or any other person for any 3rd party services, 3rd party materials or web sites.

- 3rd party materials and links to other web, provided solely as a convenience to users.

- Additional terms over financial info, environmental damage or guaranteed availability and warranty coverage.

The potential applications and end-user services developed by the C-ITS group, are scalable and descriptor detailed. To test and develop solutions, the EU Commission's 4th Working Group of 2016, brought up a group of encoded messages, ideally fitting for the purpose of recording and analyzing the privacy and data protection challenges faced by the universal connectivity deployment, applied on any potential end-user [6].

The two messaging methods, quite applicable for connected vehicles are:

- ✓ The Cooperative Awareness Messages (CAM) &
- ✓ The Decentralized Environmental Notification Messages (DENM).

On the DEN Messaging, there have been issued extensive simulations by the ETSI organization [19] (ITS technical specification report 102 637-3 V1.1.1), while considering as many parameters as possible, during an incident on the road. Some of the most crucial ones are:

- The traffic flow status
- The cause of the incident
- The sub-causes
- The linked causes
- The severity of the impact
- The basic event characteristics

The Data Elements and Data Frames carried by the DEN Messages include the following descriptors:

- **DE_messageID** (*Message type identifier assigned to the DENM*)
- **DE_generationTime** (*Time at which the DENM was generated*)
- **DF_actionID** (*Identifier generated each time an actual ITS station detects an event at a specific position for the first time*)
- **DE_dataVersion** (*Data version that indicates an update of information related to an event described by a previous DENM from the same originator ITS station*)
- **DE_expiryTime** (*Time when the information becomes invalid for further processing*)
- **DE_frequency** (*Sending frequency of the DENM as defined by the originator ITS station*)
- **DE_reliability** (*The probability of the event to be truly existent at the event position*)
- **DE_isNegation** (*Flag DE that indicates the event described by a previously received DENM from other ITS stations does not exist*)

- **DE_trafficfloweffect** (*Traffic flow situation where the event is detected*)
- **DF_situation** (*Description for the event type, including direct cause and sub cause*)
- **DF_linkedCause** (*The description of the linked causes related to the event*)
- **DE_severity** (*Severity level of the event to the road safety*)
- **DF_eventCharacteristics** (*Basic characteristics of the detected events*)
- **DF_eventPosition** (*Geographical position of the event position*)
- **DF_ refPosition** (*The reference position of the event*)
- **DE_longitude** (*The absolute geographical longitude*)
- **DE_latitude** (*The absolute geographical latitude*)
- **DE_heading** (*Orientation of the detected event, if the detected event has an orientation*)
- **DE_eventSpeed** (*Speed of the detected event when the detected event is in a mobile state*)
- **DF_traceLocData** (*Trace location referencing that describes consecutive waypoint positions leading to the event position*)

Vehicles armed with C-ITS systems able to "read" these messages, operate on a standard full status reporting data broadcast state. This broadcast complies with the overall system's function, making potential users somehow doubtful over the constant transmission and reporting.

By most researchers this is considered a vulnerable part of the system and as such, the C-ITS 4th Working Group had to undergo further evaluation. Specifically, the data transmitted over the DEN Messaging platform are considered "personal", due to possible indirect identification of individuals, if processed properly. Eventually, the European Legislation on Data Protection (94/46/EC) is actually applicable.

Moreover, in cases of C-ITS application, the "informed driver consent" cannot be missing, when certain personal data issues may arise. The optimal solution for such systems is the user authorization for manual broadcasting discontinuance, as an on-demand request, without skipping the proper warning alerts for possible adverse consequences. Further in detail, certain applications that process user-generated data without previous consent are limited in number, but their legal basis clearly defines that the respective data are not further processed or redistributed beyond their functional spectra.

4.6. Concerns over Public Motorway Readiness

The V2I and V2V environments cannot be feasible and operative exclusively in between vehicles. The obstacle in this case is not the existing technologies, the current infrastructures or the manufacturers' abilities, but the variant vehicle mix that prevails in every motorway today. Cars, trucks, buses, agricultural equipment and motorbikes, are only few elements in that mix. Interoperability among all vehicle origins has to be guaranteed in order to have a successful universal CV system.

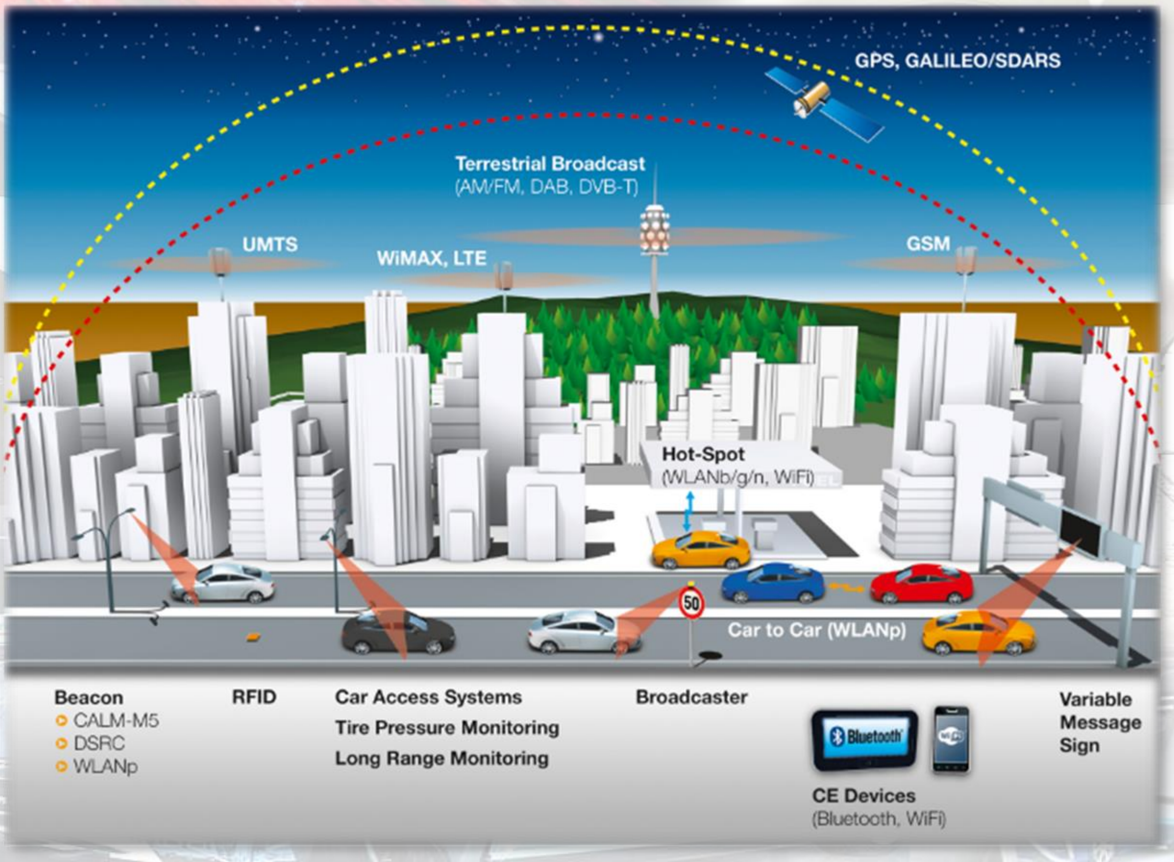


Figure 5: *The basic telematics, telecommunications and IT components required for a successful operational VANET system, among connected and non-compatible vehicles* (Continental, 2016)[34]

Many different technologies have to function in a certain combination that will provide all drivers-users with the proper information and support, in quick response, by maintaining the overall QoS characteristics at safe levels. Telecom operators that currently test communication protocols and concepts among CVs, utilize GPRS, UMTS signaling, MAN Wi-Fi, WiMAX and LTE transmissions, GPS coordinates and wideband broadcasting techniques, that interact with DSRC protocols and RFID chipsets, similar to Bluetooth channels and messaging decoders.

4.6.1. Readiness through a regular scenario

Speaking over motorway readiness, on January 14 2017, another serious incident occurred [20], this time, thankfully without any casualties or physical harm. The owner of a Tesla modes S, seized the day and wanted to drive to Red Rock Canyon in Nevada, carrying only his smartphone. Tesla offered the option of powering the vehicle with wireless key technology. The only requirement for this application to unlock and activate the vehicle was the user's smartphone and vehicle be both connected to a cellular base station (average 3G signal coverage).

The owner, having forgotten his keys home and while depending on his smartphone application, stopped the car, hopped off to check something on the rear seats, only to find himself locked outside. The Tesla's cloud server was only available when cellular signal was provided. The driver unluckily stopped by a location with no cell signal, which led to no active wireless key application. After 2 miles of walking and signal searching, he finally managed to call one of his friends, asking to bring the key fob from his home.

This is just another case, depicting that modern motorways in the U.S. are still not 100% signal supported. But the main point behind this story is the great number of secondary operational cases that are not taken into further examination, leading to functional gaps and vehicular errors, despite the high-end technology integration.

According to the C-ITS platform, service integrity and availability have to be seamlessly provided across motorways, in order to support connected and automated vehicles with no exceptions. The road ahead for the deployment is still very distant and requires a lot of additional corrective actions otherwise limited QoS shall be distributed.

4.6.2. Eligible applications supported by VANET networks

The transition from legacy vehicles to new, intelligent ones might take a few years till complete deployment shall occur. Until then – and not only for transportation matters – urban and highway traffic networks, will need a new “facelift”, as to embrace the hybrid mix of vehicles, while providing a smooth connected transportation world, no matter what the duration.

The utilization of rural, urban and motorway sectors could come up extensively useful in many vital aspects of VANETs [21]:

- Public Safety Applications
- Traffic Management Applications
- Traffic Coordination and Assistance Applications
- Traveler Information Support Applications
- Comfort Applications
- Air Pollution Emission Monitoring
- Law Enforcement
- Broadband Services and Connectivity

Considering the amount of applications these infrastructures could support, the involved stakeholders now appear to originate not just from the automotive parties and telecom fields, but also the government sections, the state authorities and the tourist and citizen protection ministries as well.

One of the major problems some of the EU governments face is the destabilized financial environment, which makes it particularly difficult to invest money catholically for road network infrastructures of that origin. Therefore it is inevitable for VANET networks to prevail soon, as they are expected to deploy only partially and with limited funding in the beginning.

Limiting the research to connectivity only issues, the Departments of Transportation under most EU countries, will sooner or later allot the cooperated telecom vendors with partial regulatory adjustment power, or in other words, granting legal authorization to propose and submit regulations for public motorway networks, regarding the rules and the actual framework that will support the connected vehicle environment.

This will in turn, enrich the telcos' operations with an extended suite of services and products, beyond exclusive telecommunication provisioning channels.

Chapter 5th

Barriers on the Framework Adoption

5.1. Legal Barriers

Cars and vehicles in general, once connected to the IoT eco-system, are attributed certain values, rather significant for their compatibility and proper operability through the web and cloud infrastructures. Those same values are also applied among other vehicles in short range. Digital handshakes, information propagation, seamless geotagging and logged records are only few of the standard device identifiers that can somehow reveal the actual vehicle's ID and activity, reliably and instantly.

The manual-to-digital transformation was deployed under the urgent need to ensure full transparency during the dominance of the World Wide Web, whether it was a matter of private usage or a Federal Bureau cyber-crime investigation case. All networking devices who meet the standards to send and receive coded or encrypted data streams, are clearly stating their origin (make) via their unique MAC address, as well as the type of technology they support.

From tower PCs to wearable gadgets and handheld devices, the network interface is always broadcasted, separating certain end-users among the mass. In the connected technology of IoT, where everything broadcasts current status and data streams, vehicles are also undergoing the same norm, therefore the same digital "rules" shall apply here as well.

The human interaction with connected cars is expected to bring up data protection issues, similar to those of laptops, tablets and smartphones. It is once again, the same type of user-machine combination.

Data originated from connected cars are according to the law considered to be "personal", when matched to an individual. But the matter here is even more complicated [22]. The question to be answered is how many drivers are going to be "authorized" to drive a certain car. A regular family of, let's say five individuals, will find it difficult to use a connected car, whenever a privacy consent notification dialogue repeats itself infinitely every time the driver is changing. There is also the problem of processing each driver's personal data separately with security and confidentiality, without perplexing driving logs among the drivers who use a vehicle.

If the consent is required, in order to activate some functions, will the authorization be demanded on every user request, when entering into the vehicle? Additionally, who are each data streams attributed to and how could the generated info put into good use [22]?

There are several parties involved in the picture such as cars' owners, 3rd party users, dealers, OEMs and component manufacturers. Most importantly, many inquiries are born as to who should have the control of data generated from connected cars. Will there be a scalable access authorization or not? Finally, in the case of non-European car manufacturers, there might be an additional intercontinental data transfer issue.

Despite issues concerning the user approach of the connected car, telecom operators and car manufacturers also seem to need a reshaping to their basic telecommunications & automotive functions that will officially apply on their products.

Indeed, if telecom vendors are meant to act as providers of electronic communication services for the purposes of telecom regulations, the issue is whether they need a license / general authorization from telecom authorities, in order to operate on connected vehicles, or not.

The applicability of telecom law obligations for an entity that is not a telecom operator will definitely trigger other law issues as well. Furthermore, such obligations might be deemed to be unbalanced against the types of data that are transferred.

Also, since most car manufacturers sell their cars globally, will they have to comply with the telecom laws of each country where their cars are sold? If not, then is it possible that a fixed law regulation will apply to all EU countries (if not to all continents globally) [22]?

The fragmentation of regulations across countries in such sectors might transform into a major barrier to the growth of such technologies on a mass production scale.

5.2. Legal Positioning of Telecom Operators and Car Manufacturers

Once inserted into the Connected Vehicle market, the car industry will sooner or later go through a reconstruction, including both product management and after-sales support among other areas.

Regarding the agreements held by car makers and software / hardware vendors, a connected vehicle is highly anticipated to follow the latest after sales support, such as new software version releases and hardware warranty, similar to the manufacturers' mechanical support for a long-term period. In cases of any manufacturing violations, connected vehicles should still get full car parts recalling procedures (steering wheel issues, airbag inspections, reported vehicle failures etc.), as happens with all motor companies for more than 20 years.

Further digital support is also expected to accompany a new connected vehicle, with car resellers being ready to offer free or low cost diagnostics, connectivity, readiness and operational inspections, once the intelligent equipment will operate quite often, whenever such a vehicle is used.

Besides any coverage, car manufacturers will also get through legal suites that comply with both mechanical and technological standards.

5.2.1. Automotive Manufacturers on a New Legal Positioning

Releasing connected car models into the market is anticipated to be escorted with segmented warranty coverage and product-user support over agreement contracts. Although modern vehicles are currently offered limited free annual service support, so far, car manufacturers only had to look after their products integrity and reliability, on both mechanical and system response and sustainability, having to worry about nothing else.

The connected car platform is closer than ever, to enrich the active values towards users and vehicles and thus, the concerns over quality and integration arise for all of the respective car makers.

5.2.2. Manufacturing Defects & System Malfunctions

Recently, several car manufacturers, such as Mercedes-Benz, Volvo and General Motors, have developed advanced software systems that automatically activate the vehicle’s braking system, in order to avoid unwanted front collisions (a mechanism for driver distraction phenomena or sudden obstacles that appear in high speed routes). Such proactive technologies would undoubtedly be included in connected and driverless cars soon.

Software or hardware manufacturing defects, usually appear in massive production lines quite often. In car companies this is a relatively frequent situation, although QC tests may come up 100% successful. Consumer protection authorities are more than just authorized, to support anyone who has had any malfunctioning products, no matter if they brought physical injuries to the users, or if the required specifications are not met.

Eventually, in cases of QC violations, specifically for connected and automated cars or manufacturing defect claims originated by end-users (buyers-drivers), researchers estimate it will take a long trip for connected car clients to prosecute manufacturers by dominance, for violations (or omissions) and product liability. The perplexed IT shape of connected vehicles will most certainly create a "safer" manufacturer environment, where in some cases any claims will somehow go under justifications attributed to user mishandling actions or damages after unofficial aftermarket parts installed.

For example, a connected or autonomous vehicle manufacturer, who performs every safety and quality control tests on its vehicles, accidentally ships one vehicle with faulty braking software or hardware. Suppose further, that this vehicle becomes involved in an accident and such accident is attributable to the fault in the braking software.

If the driver, passenger, or pedestrian is injured in the accident, they could raise a huge legal claim for strict liability arising from this manufacturing defect. The manufacturer could be found strictly liable and accused for the dangerous software fault and the passengers' great injuries, even though it exercised all possible care in preparing and shipping the product.

By the time car manufacturers initiate shipping digitally enhanced vehicles, a new legal authority should demand a second quality and control test, to be executed by the local dealers or the official distribution centers, giving the opportunity to ensure further product excellence and functionality before selling a defective vehicle. It would be ideal, having this regulation applied on all automotive makers, for as far as it is concerned, the mass market will increase the customer demand rapidly and the production lines will again have to face high productivity goals and effective QC tests while being ahead of the competition.

A manufacturer could also be subject to liability if the design of the product itself is defective in nature, although connected cars' exterior or interior design isn't expected to differ much from those of legacy and modern vehicles.

Under this risk/benefit test, a product's design is evaluated by considering the gravity of the danger posed by the design, the likelihood such danger would occur, the feasibility of a safer alternative design, the financial cost of an improved design and the adverse consequences to the consumer resulting from an alternative design. In the context of connected cars and autonomous vehicles, liability complaints alleging design defects will likely arise in connection with the shared responsibilities between the vehicle and the human occupant/driver.

Remembering the five levels of automation for connected and automated vehicles developed by NHTSA, under automation Level 2, for example, the vehicle would have systems where there exists automation of at least two primary control functions designed to work in synergy to relieve the driver of control of those functions. Further, the driver could still be responsible for monitoring the roadway and for safe operation and is expected to be available for control at all times and on short notice.

If a manufacturer markets and distributes an automated vehicle that is NHTSA level two labeled and an accident occurs involving this vehicle (because the system failed to provide the required "short notice" advanced warning), then an injured party would likely bring a system design defect cause of action. The plaintiff would argue that the vehicle should have been designed to provide more advanced warning that the driver should assume control over response times. The manufacturer might counter this argument by stating one or more of the following cases:

- The system provided sufficient warning indications, but the driver did not react timely.
- Modifying or altering the system to provide even more warning would necessitate adding costly sensors or equipment to the vehicle.
- Even if such alterations or modifications were feasible at the time of manufacture, the increase in warning time would be marginal and not make a practical difference in the driver's ability to react.

The way it looks, liability for accidents will turn into a very perplexed scheme where any legal arguments against manufacturers can relatively easily be eliminated with numerous mechanical claims or production specifications. At this point it is crucial for all parties to realize, how to handle sensitive issues with transparency and efficiency, without causing any distractions or violations to drivers and authorities.

5.2.3. Liability for Accidents on the Road

Current regulations prescribe that car owners are generally liable for accidents caused by their vehicles and are obliged to put in place an insurance coverage. However, in the special cases of connected and self-driving cars it is ambiguous whether there will be a liability frame for OEMs.

Shall this matter be contractually regulated between the manufacturers and buyers? Will these accidents fall under product liability regulations, preventing any limitation [22]?

Too many regulatory gaps will emerge, if the current legislation won't go into close examination and inevitably many amendments. Certain liability aspects include important factors like end-user involvement, passengers, connected vehicles, the public transportation network, pedestrians and the connected automation mechanisms provided by telecom vendors and automotive suppliers.

It would be extreme and strict (above law dominance) to consider loading any responsibilities to the involved drivers solely, by the time the vehicles they will use are going to be connected to the "always awaken" roads and equipped with high-end mechanisms that occasionally may fail, on unexpected vehicle or infrastructure malfunctions. It is important to split the connected transportation environment into many levels, with the framework and bylaws to apply in an adaptive way on different accident scenarios, considering priority and safety according to data logs generated by anything connected around accidents (or not).

Last but not least, local authorities will have to deal with the official and legal distribution policies of connected cars and yet again, the way to do that will go under the microscope. And this might be one of the main reasons for a late market release for vehicles of that kind. Especially when legacy vehicles may also get involved in accidents with connected ones.

All the above are just some of the legal issues that can impact connected cars and much further might arise depending on the developed technology. It will be interesting to see how car manufacturers will face such hurdles.

Once manufacturers want the data collected through connected cars to be transferred outside of the European Union, will they need an additional consent from users or rely on legal tools or not? Will the data transfer be meant to be necessary for the provision of the service in case of purchase of cars from a non-European entity?

With respect to legal battles over general responsibility for accidents, those proven obviously responsible for damages should be held accountable within the traditional legal framework, but the process of determining accurate liability can be expected to become more complicated as technology becomes more complex and the number and types of technology providers increases.

5.2.4. FURTHER CONNECTED CAR MARKET OBSTACLES

The Forbes business magazine (Forbes Inc.), listed a few important future obstacles in the connected car deployment and the legal parameters escorted by them [23]:

- Cars and vehicles in general, take longer to develop than smartphones. Cellular devices are basically information-telecommunication tools able to receive and process data. Vehicles on the contrary, are complex units with numerous sensors, different mechanical and electric components, wrapped up with a lot of different materials and can undergo quality tests in a much more timely and costly way. It will always be like that and for many more decades, the car manufacturing process will only slightly change.

- The new safety laws applied in connected vehicles will alter the connectivity policies across different platforms. The way data over connected vehicles will be managed, is expected to affect the current policies and user-agreements between telecom products and services, as governments will most definitely gain access to many more user data trails than ever before. In the U.S. and Europe, telecom related lawsuits are currently under detailed examination, considering data-sensitivity issues, the connected car platforms shall emerge.

- More and more vehicle manufacturers will be obliged to ally with telecom operators and technology firms, during the transition from legacy to connected cars production lines. The tech requirements and standards that shall prevail at that time will make it inevitable for car makers to stay out of the connected market. Although, quite a few automotive groups shook hands with ICT vendors, there are many more yet to form the rising market schemes.

- Car dealers will change the way they work, as they will have to go under new training sessions, having to familiarize themselves to the new technology equipment that will be embedded on the latest models. Apart from that, a customer that will choose to buy his / her first ever connected vehicle is going to need quick-start user directions and extra seminars, before driving the new vehicle back home safely. Official vehicle sellers are also expected to adjust their exhibition centers accordingly, in order to ensure a smooth and reliable guidance for every potential customer across the globe. It is also important to note that along different car brands, the connected platforms must not divert much between each other, for which it will be even more difficult for drivers to skip from one vehicle make to another.

Customer information should also apply on the web, with clear, comprehensible presentations and demonstrations.

Mobility and connectivity needs that are anticipated to emerge from the connected market will bring up new ways of offering more than just vehicles. In the next few years, car manufacturers will not focus only on distributing vehicles to owners, but also evaluate opportunities for profitability by leasing plans, initially in large urban environments.

On a closer examination, quite many individuals and companies would select leasing connected vehicles on a daily basis, for fulfilling their needs, leading to efficiency in traffic jammed conditions and less expenses for vehicle maintenance and ownership.

Image 20: *Dealership awareness and training sessions are expected to differ from todays' exhibitions, as the average vehicle driver is not yet deeply familiar with advanced communication or multimedia technology in vehicles (Ford's Showroom in the U.S.)* (keywordsuggest.org, 2016)[35]

Application developers are also expected to go under strict evaluation as to which of the respective applications should be included into the connectivity suites' operating systems. Built-in applications are not the only issue in this case, as certain connection protocols shall also apply on a universal scale (A2DP Bluetooth, auxiliary output, Wi-Fi link), for all carmakers and all users, if not for the most.

Another major obstacle for connected cars to penetrate the future vehicle market is attributed to the purchase policies car makers will follow for vehicle distributions. So far, potential customers were only aware of a one-off payment when purchasing a new or used car. Great inquiries are shown upon the way customers will experience the additional connectivity services payment methods. Who will financially cover any additional fees, if not the driver himself?

And what if the customers are going to have an extra charge on the data plan bill for connected car services? This will negatively affect the overall purchase experience, once established for all connected vehicle brands. As a chain effect, it will negatively affect the connected car penetration rate in the modern market, something clearly undesired.

5.2.5. Telecom operators to possess regulatory authority

Some of the communications technologies are already operating under minor or average supervision by the governments they apply on, so modern technologies are also going to be part of controlled monitoring authorities. Both cellular and fixed connections "generate" data traces that are user-attached and it is of no surprise that connected vehicles may also have their data revealed (user data, recorded footage, GPS or connectivity node locations) in possible lawsuits.

However, it is still not defined whether or not there will be any legal barriers preventing governments to access user data or not. Considering the numerous private sources from where these data may be easily retrieved, it hasn't yet been clarified if the intermediate distribution channels will be obscure to the vehicle users or not (sequential access tunneled via vehicle applications).

The United States Fifth Circuit Court of Appeals, once dealt with a special case, related to private sensitive information and access request by the authorities, under a criminal investigation. Police requested a warrantless court order to oblige cellular vendors hand over three suspects' mobile phones historical location data.

Up to this day, there are only few legal barriers, able to prevent the collection of personal data. In the connected vehicles platform, users will expect to experience a certain level of privacy, for any personal data forms, generated from their automobiles.

Under the respective U.S. Congress's Fourth Amendment [24], any investigation and legal actions should be limited in scope, providing individuals with security against unreasonable searches, as it is their right to have a privacy that shall not be violated nor mistreated. With the staged connected vehicle deployment, the prevailing barring of investigations could possibly be lifted, for further governmental access by requesting records and data by 3rd parties, “bouncing” over the legal obstacles somehow.

In short, very little regulation exists, preventing private parties from collecting, aggregating, analyzing, marketing and monetizing.

Although authorities have stated that there should be no access to private data, a different path to anonymity was proposed. Consumer Data Protection Authorities could establish a narrower cooperation with the states, demanding exclusive user-data disclosure to state citizens. That means, connected and autonomous vehicle makers to disclose to state citizens the data they collect and the uses to which that data is put, when requested (in explicit cases).

Such legislation has already been proposed in California. The Consumer Vehicle Information Choice and Control Act decided to require manufacturers of new motor vehicles sold after January 1, 2016 to make initial disclosures to the vehicles’ owners. The initial disclosures referred to the information generated and collected by the vehicle, by the time it was sold and used. The owner would have full and sole access to the information and be able to transmit it to a 3rd party with his consent. The manufacturer would not be able to take action against the owner for accessing or using the information.

In limited circumstances, a manufacturer or medical researcher could be authorized to use the collected information, only after any personal identifying information is removed.

What is left to admit, is that there may certainly occur “cases”, where OTT players and 3rd party application – telecom allies will still have level access to limited user data stacks, mostly for research and development purposes. Anonymity is not certain if will still be preserved, but if user-data access can go under limitations, the connected car deployment will take effect the soonest possible.

5.3. Legal Requirements for the IoC (Internet of Cars) Implementation

Lately, there have been significant steps towards legalizing the IoT transition from smart devices and internet services, to the Internet of Cars. Although many legislators and lawmakers have little understanding over the IoT operations and the way they are issued, car manufacturers and telecom vendors have somehow legally been defined, regarding their rebound to the fast-growing mix. The approach by the Congress in the U.S. and the governments and courts in Europe, to the governance of Connected Cars, has already given birth to standards and practices across the IoT world.

It is estimated that by 2020 there will be 250 million Connected Cars on the road and about 90 percent of new vehicles in Western Europe will probably have Internet connectivity features.

5.3.1. The SPY Car Act

On July 21, 2015, Senators Edward Markey and Richard Blumenthal proposed new legislation & bylaws (S. 1806), demanding the NHTSA merge with the Federal Trade Commission (FTC), in order to establish consumer data privacy and car computer network security rules, purposed to avoid hacking attacks in all motor vehicles manufactured for sale in the U.S.. At that time, the official 2015 NHTSA recommendations included four pillar principles in developing practical state laws for connected and autonomous vehicles [25]:

- Ensure that the process for switching from semi or full self-driving mode to manual drive is safe and simple.
- Connected and autonomous vehicles should both support features such as detecting, recording and alerting the driver on any automated system malfunction, simplifying any accident investigations.
- Installation and operation of any self-driving vehicle technologies should never overrule any federal or police safety systems.
- Self-driving test vehicles must always record and store information logs, about the status of the automated control technologies in the event of a crash or loss of vehicle control.

At the time that NHTSA issued its Preliminary Statement [26], three states had already enacted autonomous automotive legislation legalizing the operation of autonomous vehicles on public roads for the purpose of testing. These laws are substantially consistent with NHTSA's state policy recommendations.

The SPY Car Act was based on a February 2015 report over cybersecurity threats to safety and the collection and storage of driving data, including location, driving history and user data. It required collaboration between the NHTSA and the FTC to edit crucial cybersecurity standards for vehicle systems and driving data security, including:

- ✓ Strong hacking protection
- ✓ A "cyber dashboard" display label, affixed to the vehicle that describes the vehicle's compliance with cybersecurity and privacy requirements under the SPY Car Act [25]

- ✓ Fresh privacy standards including providing user awareness regarding the use and collection of data under agreement submission forms and limiting the collection use and distribution of driver-vehicle generated data by manufacturers

- ✓ A certain, up to $5,000 fine per violation, set for any violators of the SPY Car Act cybersecurity standards

The Act was developed in the U.S., but applying it in European countries wouldn't need much effort. The only demand for law re-editing would include data redistribution frameworks between EU and US manufacturers, countries and authorities. Other than that, the same digital rules apply worldwide, as happens with IoT products and services. In terms of industrial regulations everyone agrees that a national IoT strategy should be defined, able to confront all IoC stakeholders without preventing innovation and growth among continents.

The Alliance of Automobile Manufacturers published the Consumer Privacy Protection Principles for Vehicle Technologies and Services. These principles relate to the collection, use and sharing of personal and vehicle information associated with vehicle technologies that generate, collect, record and store this information. The principles call for automakers and manufacturers to ensure the following by 2017, are listed below:

- Provide consumers and end-users with clear warnings and user-selection in accepting any processing and collecting actions from system vendors, on their personal information
- Reclaim filtered personal information in a way that is transparent, legally inspected and treated within the predefined data rules which will consensually apply
- Collect information only when legally required and preserve it strictly for as long as necessary
- Apply adequate data security defenses
- Maintain the data integrity, without any alterations and provide access to users
- Take responsibilities for personal data mishandlings, according to the official principles
- Companies offering CC services along with manufacturers, have to comply with these regulations (follow the industrial bylaws). Furthermore, they have to continuously monitor enforcement activities and investigations by the related authorities, on an effort to minimize legal loopholes

In general, Internet service providers who are about to offer wireless Internet services for connected cars, will sooner or later be exposed to potential accusations and penalty lawsuits, whenever legal and cybersecurity breaches show up. The worst scenario is expected to be legal defenses when it comes to collecting consumer personal information via their wireless networks and applications. The perplexity of one or more wireless service provisioning channels among mobile users, will make it really difficult to manage the numerous actions over data privacy, considering the amount of data transmitted each time, the infinite devices running through it (smartphones, PCs, tablets, OEM consoles etc.) and the processing power needed to sustain a successfully supervised system.

5.3.2. Litigations & Trials

Consumers' Ombudsman and Data Protection Authorities in EU countries are highly expected to enforce justice, in a far stricter method, compared to how it happened so far. Many privacy and security lawsuit cases have been filed, defending manufacturing issues on numerous early connected vehicle models. More in detail, actions have been filed to many American federal courts, spotting distinct security vulnerabilities, able to be exposed via the CAN system.

Posing these statements against security matters, prosecutors claimed it is easy enough to penetrate the minor firewall of the vehicle's system and gain access to stored current and historic data, leading to remote control and monitoring (steering, braking, acceleration, etc.). This claim was based on the manufacturing standards of any relevant OEM equipment that was by default installed in a connected vehicle. Other accusations included possible imminent breaches of warranty and violations of consumer protection laws by the existing hackable vulnerabilities.

In the majority of those cases, car manufacturers attempted to dismiss the claims, by posing the fact that no physical injury ever occurred, neither any of the prosecutors were victims of data interceptions or remote vehicle control. Also, it was officially announced that basic level connected car data could never cause a serious invasion of privacy, due to their descriptors and purposes. In California, a similar accusation filing was closed by naming the alleged – possible injuries as unproven ones. The court agents separated certain data elements that could be combined in order to identify unprotected security threats. These elements were:

- The driver
- The vehicle's performance
- The location data from Social Security Numbers
- The credit card numbers

Eventually it was proven those data were not protected under the Californian privacy laws.

Similarly, other plaintiffs were dealing with the manufacturers' infotainment systems, claiming there was limited to no protection between the CAN link and the engine control units on the embedded systems they distributed. As mentioned earlier, wireless radio connections could provide hackers with targeted remote access, thus many future cases may come up, if manufacturers won't prepare their in-car systems with strong security barriers.

In such cases, both sides will have to bring factual and tangible testimonies, in order to provide the court with full transparency and the ideal bylaws for the upcoming connected vehicles legal framework.

Therefore, manufacturers will definitely be required to hand over historic data and driver logs (equivalent to the actual system time a security threat was detected), whenever requested to. On the other side, drivers and users in general will be demanded to prove their claims through very detailed reports and with the proof of being widely aware of such a vehicle's connectivity and automation mechanisms / systems.

5.3.3. IMPACT & SEVERITY ON THE REGULATORY FRAMEWORK

The constantly updated regulatory framework, leads to relative doubt and limited stability over regulations for technology companies, automotive groups and manufacturers in general. Most production and manufacturing plants are always forced to comply with the latest litigations and legislative developments, ensuring their products are legal, safe and distributable around the globe.

Due to both connectivity and security requirements, it is nowadays severely complicated for mass production corporations to follow multiple law enacts in line with sustaining a proper product or service form. The extra complexity arises whenever these products follow hard-to-violate standards and constant quality testing.

From the software and hardware inners of a vehicle till the final exterior design, all those legal restrictions add extra effort for manufacturers to keep their products legitimate and up to date. Considering connected cars, the important part for a successful legal morphing should only include legislations that apply on the substantial part of a CV platform. This will be the key to support automotive and tech combinations without perplexing the legal framework or stuffing it with infinite bylaws that may even apply in a different way between manufacturers or vehicle models.

The CV stakeholders may set as their first priority, an engagement of safety specifications and digital security on the developing platforms, setting value-added services on a secondary level. Both connected and automated vehicles shall never get themselves promoted & released in the car market, based on what services they offer. Instead they may positively affect the market, only if they enter the potential customers' trust and confidence sphere on new technologies, be easily applicable on any scope.

Production companies should remain vivid and awake in monitoring any enforcement activities, cybersecurity ruling and vulnerabilities eliminations, shaping their vehicles and tech-components accordingly. In addition, regulations applied in CVs should also constrain software and connectivity vendors to minimize data volume, as the next years will be crucial, in terms of processing efficiency, managing Petabytes and unbelievable amount of information on the IoT world.

European and American Departments of Transportation, have lately expressed their decisions over states wishing to apply licensed operators to initially lead the way, by supervising any "connected" cockpit safely, with the ability to immediately assume control over the vehicle during all testing on public roads.

State regulatory bodies require testing and quality authorities to submit official plans, demonstrating their efforts to minimize risk to others. They also seem to require instant crash-reporting mechanisms and vehicle overriding operators, to assume control in unwanted cases of failure on connected and automated systems.

Chapter 6th

A Promising Future

6.1. Suggestions for a Smooth Connected Vehicle Platform Release

Summarizing, in order to harmonize the forces that will shape the connected car market, many key legal issues have to be documented and reconstructed, after thorough examination. In a market where newcomers will await to experience the advanced vehicles and legacy vehicle owners will go through a significant alteration of the way they faced their cars, every CV level must be completely enacted according to official directives, applicable on every end-user without variations or discriminations.

From substantial e-Call services to the data transaction between nations, these are the leading factors that can assist smooth and homogenous CV platform deployments [29]:

- Electronic Communications Sector
- Regulations for drivers in CVs and AVs
- Telecommunications and data protection mechanisms
- Manufacturing standards
- Privacy and security issues
- Cross-border transfer restrictions

6.1.1. The Electronic Communications Sector

The electronic communications sectors include certain actions like data roaming between mobile devices and interoperability between different grounds.

While the connectivity expands into vehicles, as said, cars will be dealt like smartphones, only bigger. Therefore, issues such as ownership of vehicles, additional fee charging and possible restrictions may issue. Also, concerning the MVNO trend [27], essential operational requests will have to be adjusted. An example would be the connectivity status of a vehicle, moving from a mobile network operator to a virtual one (usually applied across neighbor countries). Other requests will demand high vehicular response transition between mobile cells or base stations, while on high speed trips, in order to avoid dangerous blank connectivity periods.

Currently Ericsson, SK Telecom and BMW Group Korea are working on eliminating this barrier, by achieving data speeds of 3.6Gbps, on test-vehicles running above 170km/h. The radio transmission points on the testing area reached 1.5Gbps throughput in the 28GHz band, while data transmission was switched from one aggregation point to the other [30].

E-Call services and emergency vehicle geo-positioning are also few key elements of that sector and must be developed with strict functional ranges, serving solely the purposes they are developed for, excluding any location logs records or other actions without user permission (Directives 95/46 & 2002/58).

6.1.2. Regulations for Drivers

Equipping vehicles with additional in-car alarms and notifications makes it difficult for drivers to focus on the road, surrounded by displays and dashboards with pop-up messages. It is vital for connected vehicles to be adapted to specific user profiles that will ensure no distractions shall happen while driving a vehicle [29]. Following such user-policies includes both the human factor and the embedded applications that will generate the messages and alarm info.

Including other cases as well, automated vehicles that are of low level automation, should run under different law frameworks than fully automated ones, since requirements alter between automation degrees. Additionally, between legacy and connected vehicles, possible interactions and accident cases are expected to reshape, as a matter of justice and right accusations over offences, liability and insurance coverage conditions.

6.1.3. Telecommunications and Data Protection Mechanisms

Telecom vendors must be detailed when providing CV services, mostly for road safety, traffic - vehicle management and cooperation with state and municipal authorities. The aim is to design an effective system that will not only provide the spectrum and connectivity range for CVs, but also help the army, the police and inspection teams, track suspects and hostile truckloads effortlessly and at the right time.

New road laws will need to be edited, for vehicles that are not following technologic standards (referring to the after-deployment phase), whilst violations should also undergo a different appreciation. Other cases for telecom services reconstruction may also include redesign of the available connectivity contracts for end-users, as an agreement that will help both application parties and governmental authorities, for terrorism avoidance and surveillance purposes, such as FBI or CIA purposes, on a national security level.

6.1.4. Manufacturing Standards

Vehicle manufacturers are deeply vulnerable, considering the production lines and the economic impact, caused by the connected car technology. But vehicle manufacturers are not the only players that have to get their products under a consideration. Motorway and urban connectivity equipment incorporations shall revise the infrastructures they will apply on public areas, complying with human health standards and legal operations of short range radio networks between RSUs and OBUs.

Following the respective legal frameworks of each country, telecom components have to be certified over the transmission power they utilize, the energy consumption and antenna radiation levels. Especially on DSRC protocols and near field connectivity, low energy Bluetooth sensors and NFC circuits would be ideal for public infrastructure without hazardous consequences for pedestrians, drivers-passengers and neighbor buildings.

6.1.5. Privacy, Security and Cross-border Restrictions

Data privacy laws include any recording and disclosure of user-data, based on absolute rules. Application and system developers need to cooperate with the respective government departments in order to categorize which information should be handled with complete confidentiality, as well as which of the data will offer partial or total user identification.

Data Protection Authorities must also initiate examining CV data flaws, for further research conclusions, like data protection filings and security breach notifications, under contracted terms between application databases and end-users (licensing, user rights, vendor responsibilities etc.). National implementations of the Data Protection Directive may need additional amendments, as technology evolves. Additional regulations and bylaws are important for modern data technology systems, especially regarding Data Regulations [29].

Moreover, although many EU states have already approved specific regulatory frameworks, others are not yet included, nor are they aware of these technologies yet. It is crucial to have the E.U. commission synchronize national actions among countries, in order to not only distribute executive orders in some of them, but have them all enacted into connected and autonomous vehicles, making the overall deployment less complicated and more manageable.

6.2. Conclusion

Currently, many motorways around the globe are equipped with sufficient optical fiber networks and high-speed wireless transmission units, but the appropriate CV interfaces are still under research and development. Numerous sub-cases have to be identified and eliminated under constant testing of connected vehicles on any possible everyday scenarios.

Every radio-telecom related bylaws edited until today contain every single aspect of the legal substance between telecom systems and transmission principles. With the telecom-automotive convergence, new rules will have to apply on both vendors and users, confronting both sides with sufficient legal and law support.

Many telecom regulations are expected to remain as are, ensuring user safety, legal radio transmissions and signal coverage equal to the physical and technical standards followed by telecom operators. Others will adjust to the upcoming issues that may appear from the IoT world.

Once CV platforms get adopted by governments, new market approaches will show up, reconsidering the way products and services are distributed. Also new municipal and state authorities will morph the procedures through which such services will be inspected and legally manipulated.

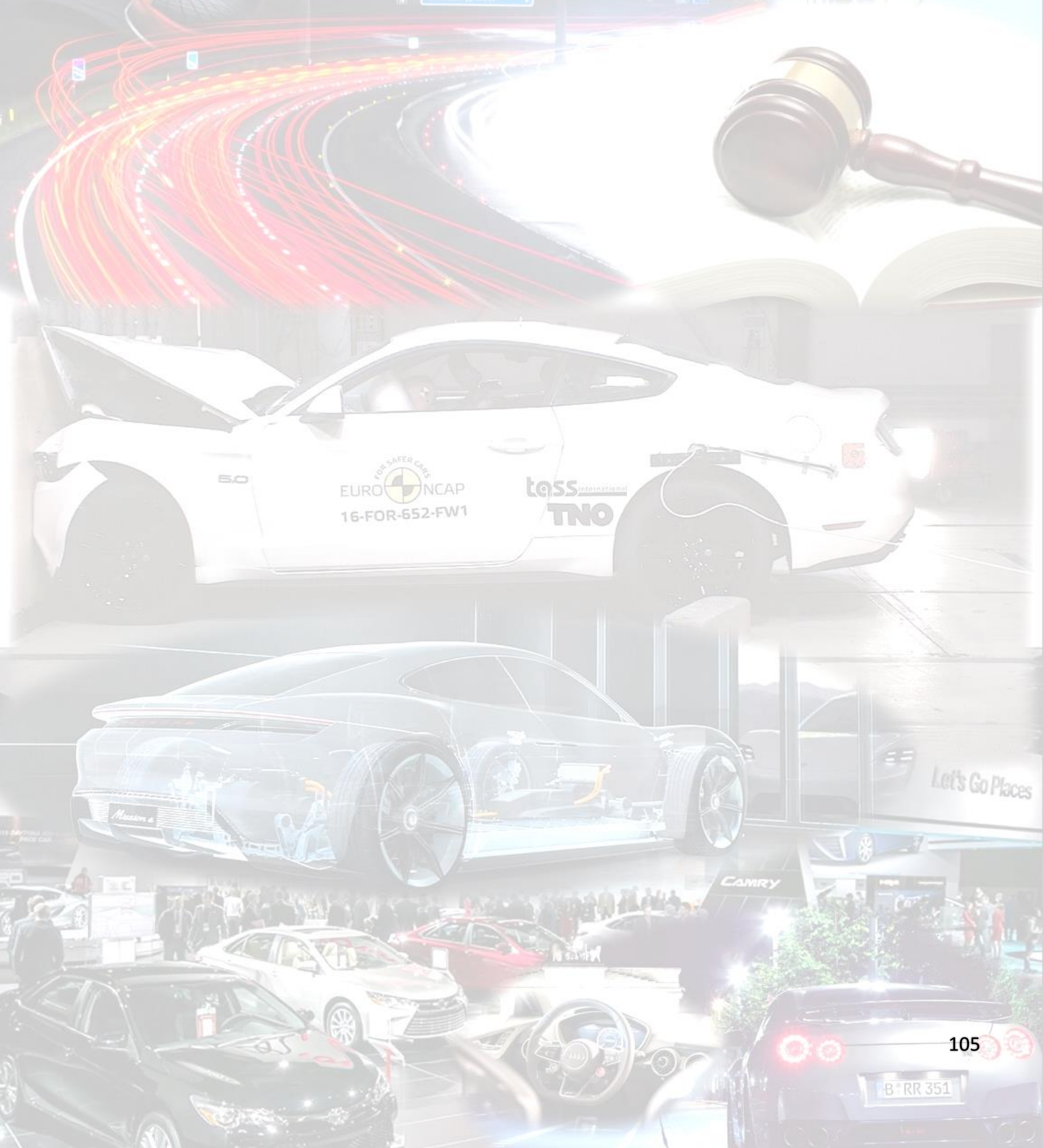
Once the EU Commission and authorities finalize their running projects and working groups, a lot of procedures will alter, leading to a modern, more human-oriented distribution of services, able to slowly engage connectivity mechanisms that will enhance everyone’s life, equally and within the safety and security contexts.

The IoT dominance is already on a satisfying level, showing the way for cars to operate into this world wide connected network, just like any other internet devices does. In the next decade, it is expected for vehicles in general to equip with artificial intelligence cores, ready to take action without human interference.

Motorway networks are steadily transforming into smart ones, able to support applications and services that are vehicle-oriented. It's the only way to eliminate fatal speeding accidents and reduce CO_2 emission, visualizing greener, more "clever" route networks, always at the drivers' and passengers' service.

Technology is applied into every individual's lifestyle, serving better practices on regular everyday scenarios, in a way to positively support social and private initiatives. By approaching the human behavior, technology should always serve the humanity on good purposes, providing undeniable security and privacy and with no individual privilege violations.

The next 5 years will be crucial for the massive connectivity transformation, considering the globalizations' wide diffusion. Markets are already planning on their next targets and the near future is brightly promising.



Bibliography

[1] A. B. & M. Safar, "Ambient Technology in Vehicles: The Benefits and Risks," Procedia Computer Sciene & Elsevier, Kuwait, 2016.

[2] Strategy&, PwC, "Connected Car Report: Opportunities, risk and turmoil on the road to autonomous vehicles," PricewaterhouseCoopers , Germany, 2016.

[3] M. M. L. M. S. Ilgin Guler, "Using connected vehicle technology to improve the efficiency," Elsevier Ltd., ETH Zurich, Switzerland, 2014.

[4] A. C. P. D. S. F. F. Adriano Alessandrini, "Automated Vehicles and the Rethinking of Mobility and Cities," Elsevier, Rome, 2013.

[5] COSMOTE S.A., "www.cosmote.gr," 2016. [Online]. Available: https://www.cosmote.gr/fixed/corporate/media-center/news/details/-/asset_publisher/wpF6f9kWWozl/content/smart-parking-smart-lighting-στη-χαλκιδα. [Accessed 25 November 2016].

[6] European Commission, "C-ITS Platform," European Commission, European Union, 2016.

[7] H. W. T. K. a. K. C. Robert L. Bertini, "Preparing a Roadmap for Connected Vehicle / Cooperative Systems Deployment Scenarios: Case Study of the State of Oregon, USA," Elsevier Ltd., San Luis Obispo, CA, USA, 2016.

[8] P. I. S. R. Simon Minelli, "Evaluation of connected vehicle impact on mobility and mode choice," Elsevier Ltd., Ontario, 2015.

[9] K. K. Daniel J. Fagnant, "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations," Elsevier Ltd., Salt Lake City, 2015.

[10] McKinsey & Co., "http://www.mckinsey.com," 2016. [Online]. Available: 12. http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car. [Accessed December 2016].

[11] Patrick Mutabazi, "https://www.linkedin.com," LinkedIn, [Online]. Available: https://www.linkedin.com/pulse/how-telecoms-companies-can-capitalise-growing-car-patric-mutabazi. [Accessed December 2016].

[12] http://www.acea.be, "http://www.acea.be," November 2016. [Online]. Available: http://www.acea.be/press-releases/article/37-leading-companies-join-forces-in-european-automotive-telecom-alliance. [Accessed 2016].

[13] Federation Internationale De L'Automobile, "What Europeans Think About Connected Cars," FIA Region I, Brussels, 2016.

[14] www.wired.com, "https://www.wired.com," 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway. [Accessed October 2016].

[15] www.theguardian.com, "https://www.theguardian.com," September 2016. [Online]. Available: https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes. [Accessed October 2016].

[16] R. D. P. Paolo Cencioni, "A mechanism to enforce privacy in vehicle-to-infrastructure communication," Elsevier Ltd., Rome, 2007.

[17] A. R. L. G. A. C.-P. S. Sicari, "Security, privacy and trust in Internet of Things: The road ahead," Elsevier Ltd., Varese / Bari, 2014.

[18] "http://www.apple.com," Apple Inc., [Online]. Available: http://www.apple.com/legal/internet-services/itunes/appstore/dev/stdeula/. [Accessed October 2016].

[19] ETSI, "www.etsi.org," September 2010. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/102600_102699/10263703/01.01.01_60/ts_10263703v010101p.pdf. [Accessed October 2016].

[20] "http://www.telegraph.co.uk," January 2017. [Online]. Available: http://www.telegraph.co.uk/technology/2017/01/16/tesla-driver-stranded-desert-smartphone-app-failure/. [Accessed February 2017].

[21] D. J. Pu, "How Vehicular Ad hoc networks Serves Smart City," Beihang University, Bejing, 2013.

[22] G. Corragio, "http://blogs.dlapiper.com," October 2014. [Online]. Available: http://blogs.dlapiper.com/privacymatters/connected-cars-legal-issues-and-hurdles/. [Accessed November 2016].

[23] F. Inc., "www.forbes.com," 2016. [Online]. Available: https://www.forbes.com/pictures/mkk45ihlk/10-obstacles-for connected-cars/#13b974fc12bb8. [Accessed 2017].

[24] Wikipedia, "en.m.wikipedia.org," [Online]. Available: https://en.m.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution. [Accessed February 2017].

[25] R. B. Edward Makrkey, "https://www.markey.senate.gov," June 2015. [Online]. Available: https://www.markey.senate.gov/imo/media/doc/SPY%20Car%20legislation.pdf. [Accessed December 2016].

[26] A. C.-T. William J. Kohler, "Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles," Santa Clara High Technology Law Journal, Santa Clara, 2015.

[27] S. Tassis, "www.geeklawdigest.gr," July 2016. [Online]. Available: http://www.greeklawdigest.gr/topics/technology-media-electronic/item/81-electronic-communications-legal-framework-guide. [Accessed February 2017].

[28] EETT, "http://www.eett.gr," [Online]. Available: http://www.eett.gr/opencms/opencms/EETT_EN/. [Accessed November 2016].

[29] Baker McKenzie, "http://www.bakermckenzie.com," October 2015. [Online]. Available: http://www.bakermckenzie.com/-/media/files/insight/publications/2015/10/global-issue-spotting-for-automotive-parts/pn_oesa_regulatoryissues.pdf?la=en. [Accessed February 2017].

[30] Piotr Pietrzyk, "Ericsson, SK Telecom and BMW Korea achieved downlink data speeds of 3.6Gbps with driving speeds of 170Km/h," LinkedIn, 2017.

Bookmarks - web sources

1. http://trafficsafe.org/index.php/intuitive-clarity-jaguar-connected-car-experience-8143/
2. Ambient Technology in Vehicles: The Benefits and Risks (*Ahmad Bennakhi and Maytham Safar / Procedia Computer Science 83 (2016), pg. 1062*)
3. http://www.continental-corporation.com/www/pressportal_com_en/themes/press_releases/3_automotive_group/interior/press_releases/pr_2016_09_01_telematics_20-years_en_us.html
4. Connected Car Report: Opportunities, risk and turmoil on the road to autonomous vehicles
5. http://www.caranddriver.gr/audi/arthro/audi_a3_sport_sedan_stin_ellada_apo_23_040_videos-7286193/
6. http://www.dailymail.co.uk/sciencetech/article-2539498/Audi-shows-smart-car-mean-never-stop-red-light-again.html
7. http://telematicsnews.info/2014/04/02/tesla-chooses-telefonica-for-connectivity-across-europe_a524/
8. http://www.lifo.gr/now/greece/121506
9. http://www.autotalk.com/global-auto-execs-now-embracing-autonomous-and-connected-car-technologies-31601/
10. Ambient Technology in Vehicles: The Benefits and Risks (*Ahmad Bennakhi and Maytham Safar / Procedia Computer Science 83 (2016), pg. 1059*)
11. http://money.cnn.com/2016/07/13/luxury/model-x-60d/

12. http://www.hardwarezone.com.sg/tech-news-intel-collaborates-power-connected-transport-platform-solution & http://www.androidpolice.com/2014/04/30/automatic-link-review-the-one-nag-whose-yammering-might-actually-improve-your-driving/
13. https://www.cbinsights.com/blog/startups-drive-auto-industry-disruption/
14. http://connected-car.mybluemix.net
15. https://www.slashgear.com/audi-urban-future-explores-connected-self-driving-cars-11324821/
16. http://www.forbes.com/sites/kbrauer/2016/03/02/top-10-autonomous-car-facts-when-will-self-driving-cars-arrive-whats-holding-them-up/#212b689b4f1a
17. http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car
18. https://epthinktank.eu/2016/01/11/automated-vehicles-in-the-eu/
19. https://electrek.co/2016/06/30/aftermath-rare-rollover-tesla-model-s-crash-truck-video/
20. Preparing a Roadmap for Connected Vehicle/Cooperative Systems Deployment Scenarios: Case Study of the State of Oregon, USA (*Roadmap for Connected Vehicle / Cooperative System Deployment Scenarios R. Bertini at al., pg. 449*)
21. Preparing a Roadmap for Connected Vehicle/Cooperative Systems Deployment Scenarios: Case Study of the State of Oregon, USA (*Roadmap for Connected Vehicle / Cooperative System Deployment Scenarios R. Bertini at al., pg. 451*)
22. Preparing a Roadmap for Connected Vehicle/Cooperative Systems Deployment Scenarios: Case Study of the State of Oregon, USA (*Roadmap for Connected Vehicle / Cooperative System Deployment Scenarios R. Bertini at al., pg. 453*)
23. Preparing a Roadmap for Connected Vehicle/Cooperative Systems Deployment Scenarios: Case Study of the State of Oregon, USA (*Roadmap for Connected Vehicle / Cooperative System Deployment Scenarios R. Bertini at al., pg. 455*)
24. Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations (*D.J. Fagnant, K. Kockelman / Transportation Research Part A 77 (2015), pg. 169*)
25. http://beaudaniels-illustration.com/Generic-car-web-2015/Vehicle-sensors.html
26. http://www.thedetroitbureau.com/wp-content/uploads/2014/10/Audi-RS7-Piloted-Concept-schematic.jpg

27. https://www.slideshare.net/mobile/M2MTelefonica/20150526-io-tfleetnicejmcaramesvf

28. FIA Survey Brochure 2016 (*What Europeans Think About Connected Cars, pg. 11*)

29. FIA Survey Brochure 2016 (*What Europeans Think About Connected Cars, pg. 15*)

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

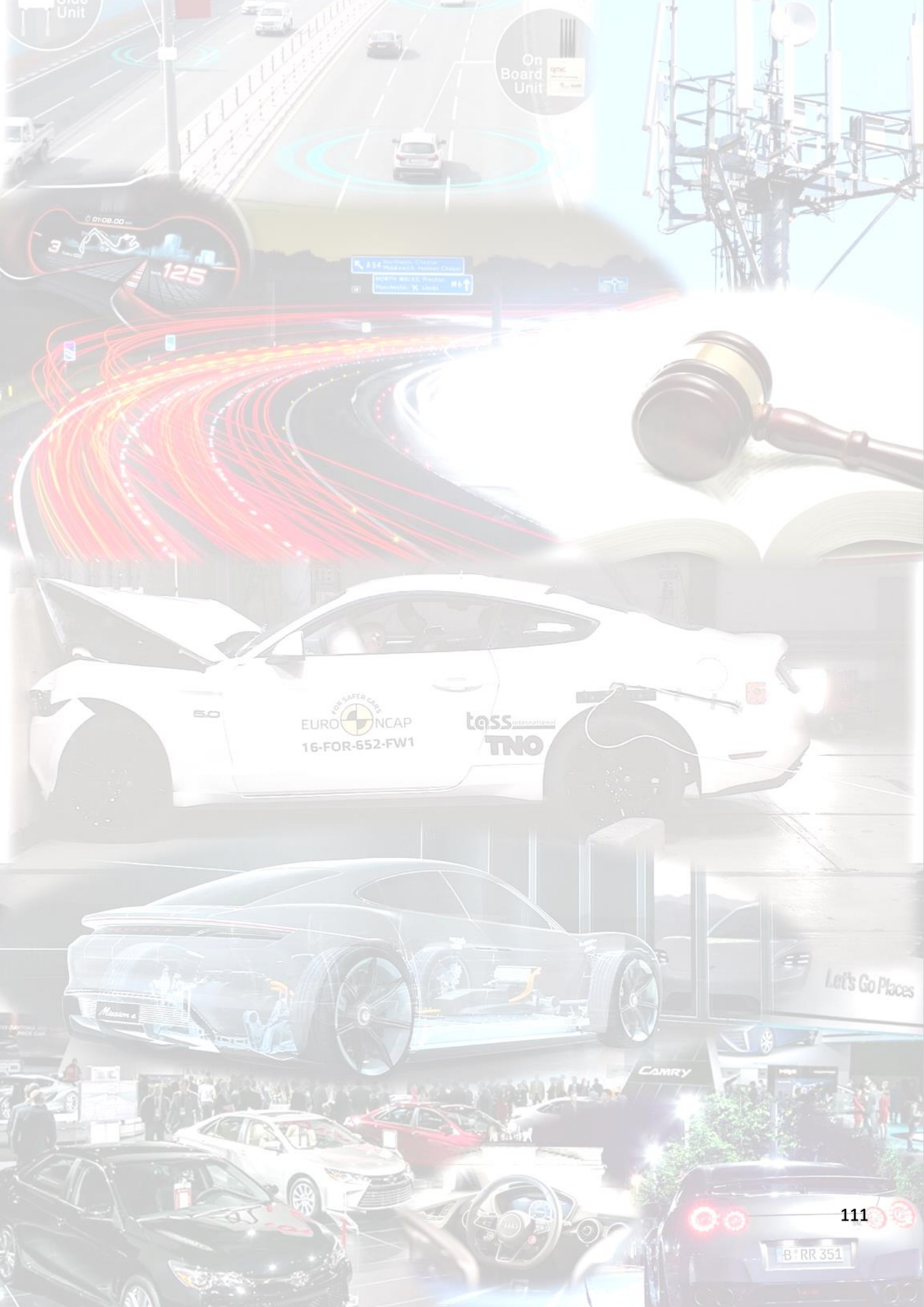
31. http://analysis.tu-auto.com/autonomous-car/us-government-gets-gear-investing-connected-cars

32. http://www.bakermckenzie.com/-/media/files/insight/publications/2015/10/global-issue-spotting-for-automotive-parts/br_automotive_connectedcar_nov15.pdf?la=en

33. http://www.a2z-support.com/apple-carplay/ & http://www.androidpolice.com/topics/android-os/android-auto/

34. http://www.continental-corporation.com/www/pressportal_com_en/themes/press_releases/3_automotive_group/interior/press_releases/pr_2014_03_27_lte_en.html

35. http://keywordsuggest.org/gallery/522424.html


On
Board
Unit
125
EURO NCAP
16-FOR-652-FW1
TNO
Let's Go Places
CAMRY
B RR 351