The Five Core Elements of Changing Mobility

AMO Labs CEO / Sim SangGyoo, Ph.D

CONTENTS

SPACE?

The Internet of Things (IoT) and the Cloud — these buzzwords have broken out of IT circles and made it mainstream. Driving the fourth industrial revolution, the two technologies power the connected devices that will enable transformational change in our society across multiple industries. Already, a network of devices, cars, home appliances and other "things" are capable of transmitting and exchanging data through software and connectivity. However at the center and the beginning of change lies one of them — the automobile.

Source : space.com

Cars have continuously evolved, starting with the commercialization of steam engines in the late 18th century, followed by the introduction of cars with internal combustion engines running on fossil fuels at the end of the 19th century. Cars have now become daily necessities that make mobility faster, safer, and easier than ever before. However, recent advancements have truly made us push the boundaries of a car in a way that makes flying cars or submarine cars no longer seem a thing of distant fantasy. In February 2012, a car entered outer space when Elon Musk launched a Tesla Roadster on a SpaceX rocket.[1] More

[1] https://www.space.com/39633-spacex-tesla-roadster-starman-final-photo.html

than just a novelty, Musk's stunt opened eyes to change by taking a car far outside its perceived boundaries.

The word "space" has two meanings: it can refer to outer space in the cosmic sense, or a place or room in the spatial sense. When it comes to cars, there's a tight connection between mobility and the concept of space. Cars provide us with the mobility necessary for seeking new living space, and as we drive from one place to another, cars themselves serve as living spaces in that journey. We've now even witnessed a car reach beyond the spatial boundaries of Earth and enter into outer space.

Aside from sending cars to space, Elon Musk is also well known as the head of electric car manufacturer, Tesla. While merely a thing of films or fantasies in the past, these days, it's not difficult to spot electric cars on roads. If we include hybrid cars and plug-in hybrids in our definition, electric cars have actually become quite common in today's car market. This is not the only clear shift in the car industry.

Security
Platform
Autonomous
Connectivity
Electrification

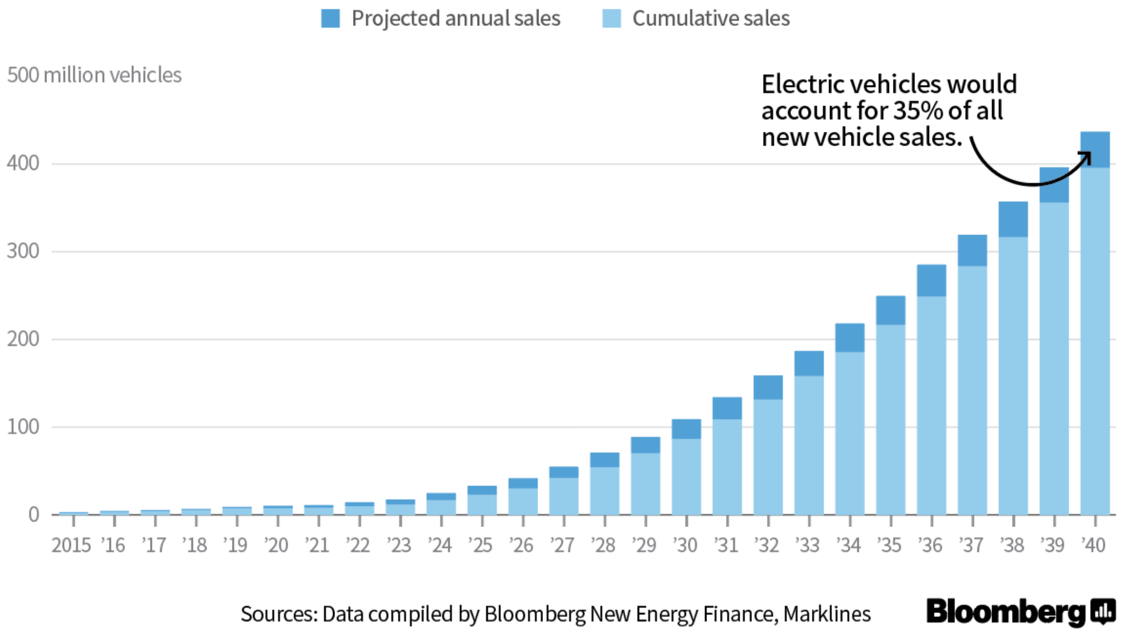
In addition to its conventional meanings in the spatial and cosmic sense, "SPACE" may also capture the five core elements of changing mobility: Security, Platform, Autonomous, Connectivity, and Electrification. These five concepts form the technical foundation of smart cars, or what many might like to call "cars of the future".

Electrification

The governments of France and the United Kingdom recently announced a ban on the production of all gasoline and diesel cars by 2040.[2] Similarly, the Netherlands has confirmed a ban on fossil fuel-burning cars by 2030, and Germany is also in talks to end the production of new gasoline and diesel cars by 2030.[3] Automobile manufacturer Volvo has vowed to stop designing solely combustion engine-powered cars by 2019.[4] According to data compiled by Bloomberg, electric cars will account for 35% of all new car sales by 2040.[5]

The Rise of Electric Cars

By 2022 electric vehicles will cost the same as their internal-combustion counterparts. That's the point of liftoff for sales.



Electric vehicles would account for 35% of all new vehicle sales.

Sources: Data compiled by Bloomberg New Energy Finance, Marklines

The move to electric cars makes sense. Electric cars use a combination of batteries and electric motors for a light and compact form. This provides a significant advantage over cars with internal combustion engines that require powertrains to generate power and get wheels spinning. Two important factors that determine the convenience and performance level of a smart car are battery capacity and charging time.

[2] http://global-autonews.com/bbs/board.php?bo_table=bd_008&wr_id=2387

[3] http://thegear.co.kr/15232

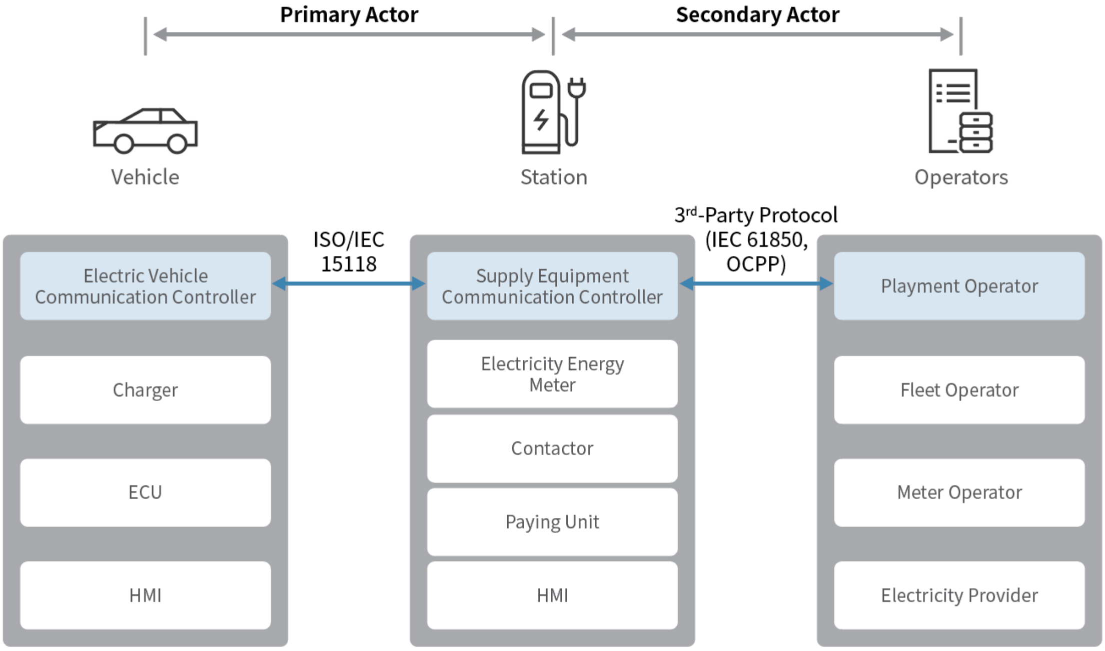
[4] http://www.autodaily.co.kr/news/articleView.html?idxno=336321

[5] https://www.bloomberg.com/features/2016-ev-oil-crisis/

Here, many mistake charging for a simple task of filling up the car's internal battery. In reality, the charging process of a smart car does not exclusively involve the transfer of electricity, but also the transmission of data. This is comparable to how smartphones are capable of both charging and data transfer once connected to a computer.

Therefore, charging cables of electric vehicles should be recognized as new communication channels. For example, while the car is charging, the transaction cost is automatically calculated and paid via communication between the vehicle and the charging station. Such a charging system is referred to as Plug&Charge or Plug&Pay. Once wireless charging technology advances to a point where electric cars can be charged while driving, Plug&Charge is expected to become an even bigger game changer in the electric vehicle industry.

New opportunities can also be found in the time spent charging an electric vehicle. The average charging time is not measured in seconds but minutes, and occasionally even hours. During charging, the car and the charging station are capable of engaging in stable communication, which means this time can be used for analyzing diagnostics or updating the car's software. In other words, charging equipment can simultaneously provide the car with electricity and keep it up to date.



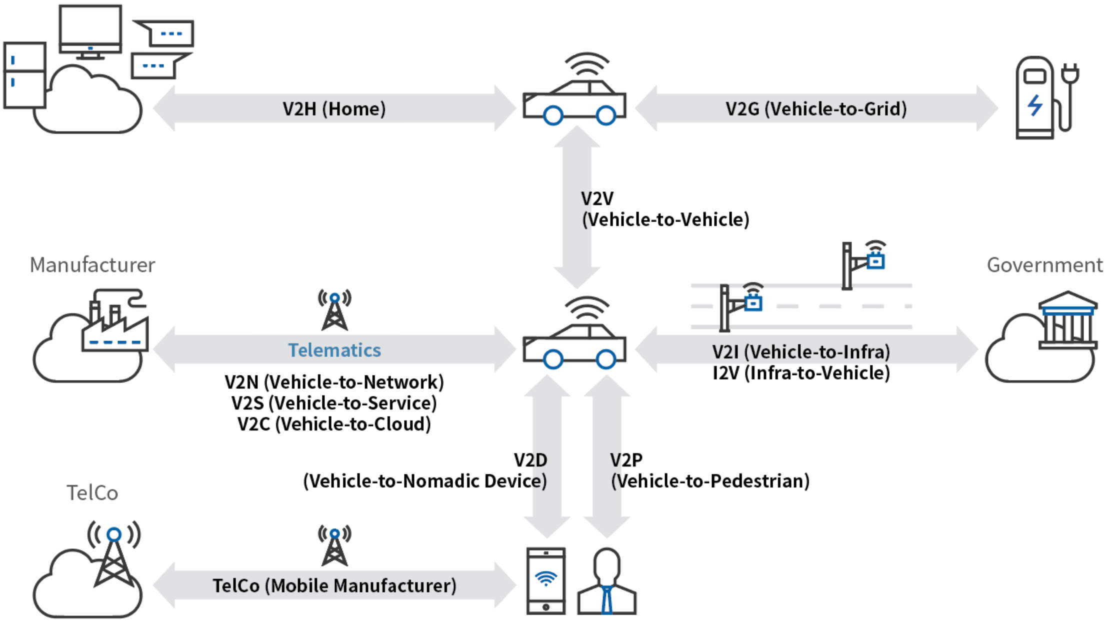
However, one must note that any communication between vehicles and charging stations, as well as charging stations and charging-related service providers (or secondary actors), must take place under a secure connection. At the very least, all entities in a communications link must perform mutual authentication, all confidential data must be encrypted, and all data that require authentication and assured integrity must be secured using electronic signatures. Security measures must be applied also to provide a secure payment system and ensure the reliability of services provided by secondary actors.

Connectivity

9

What sets IoT devices apart from conventional gadgets is their extent of connectivity. Similarly, connectivity is what differentiates a connected car from a conventional car. That is not to say traditional automobiles are not connected. After all, making a phone call or listening to music by linking a smartphone to a vehicle via Bluetooth is an example of connectivity. Opening car doors using a mobile app or accelerating using telematics software are also examples of mobile communication enabled by telecommunications services.

However, connected cars deliver a significantly higher degree of connectivity in comparison to traditional vehicular networks and cars. This connectivity includes communication among vehicles called V2V (Vehicle-to-Vehicle), communication among vehicles, roads, and other infrastructure called V2I (Vehicle-to-Infra), communication among vehicles and electrical grids called V2G (Vehicle-to-Grid), communication among vehicles and various mobile devices called V2D (Vehicle-to-Nomadic Device), and communication among vehicles and smart home sensors called V2H (Vehicle-to-Home). The latest new model to emerge is V2P (Vehicle-to-Pedestrian) which refers to communication among bicycle or motorcycle users, pedestrians, and vehicles. Automobile manufacturers are now looking to utilize cloud and web-based technology to provide new services with effortless connectivity, which would allow for more holistic services than traditional telematics. Such communication models are referred to as V2N (Vehicle-to-Network), V2S (Vehicle-to-Service), or V2C (Vehicle-to-Cloud).



As explained earlier in the Electrification section, the V2G model includes services provided via connectivity between secondary actors and electric cars connected to charging equipment.

Some household appliance manufacturers, such as Samsung Electronics, are trying to connect the car with smart refrigerators and smart TVs in an attempt to gain leadership in the V2H market. For example, at the 2016 Consumer Electronics Show (CES), Volkswagen and LG Electronics put on a demonstration on how to connect cars with refrigerators. More recently, focus has shifted to voice recognition technology and smart speakers, a market currently dominated by Amazon's Alexa. This synergy between mobility, IoT and voice recognition technology was showcased at the 2018 CES, where we could see not only cars but all kinds of IoT products compatible with Alexa. There, Alexa and Amazon Cloud served as intermediaries supporting seamless connectivity between vehicles, other IoT devices, and the home hub. Similar integrations have been proposed by Apple (CarPlay) and Google (Android Auto), which are working on allowing cars to easily connect with other devices using Apple Cloud or Google Cloud.

From a government perspective, the most interesting opportunities are provided by the V2V and V2I models. They can be utilized to increase safety on the roads: V2V communication has potential in preventing car collisions, whereas V2I technology can help create a more secure driving environment by providing relevant parties with real-time traffic information. Based on V2V and V2I communication, C-ITS (Cooperative Intelligent Transportation System) technology is revolutionizing traffic infrastructure all around the world. In the near future, the V2P model is expected to be integrated into the next-generation traffic infrastructure.

Many automobile manufacturers are pushing the V2C/V2S models along with the V2H model, which can provide information required to create new, valuable business opportunities by transforming cars from being simply a means of transportation to becoming spaces for service consumption. These services play a significant role in shaping the Platform aspect of the next-generation car framework, or SPACE, as dubbed in this paper.

Cars of the future are broadly labeled "smart cars." But what exactly does it mean for a car to become smart?

It means that cars themselves will become smart devices. Most of us already own at least one smart device: a smartphone. For a moment, imagine smartphones without connectivity, and particularly without Internet connection. Taking this even further, what if personal computers couldn't connect to the Internet? One would probably wonder what to do with these devices, but it is no different with the latest smart device: the smart car. Connectivity is key in transforming regular cars into smart cars.

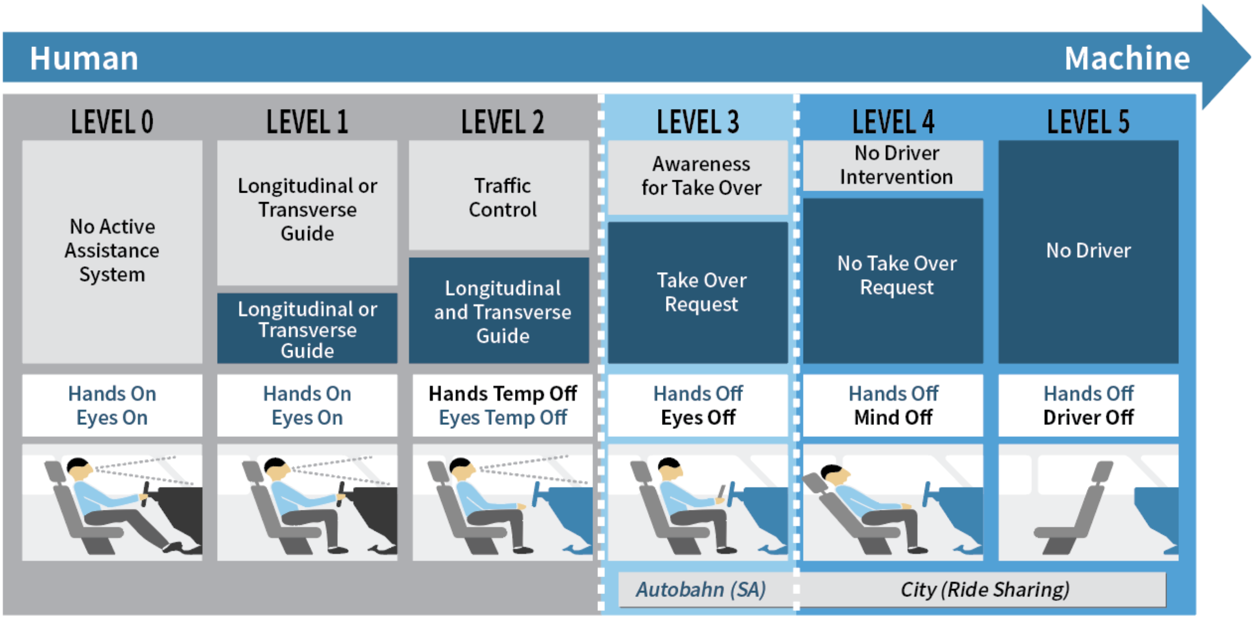
While connectivity is important in making the car more practical and secure, connectivity also makes the car more vulnerable due to more exposed communication channels. This opens up the possibility of system interruption due to data tampering by an untrusted party, or loss of system control due to a hacking attack on exposed channels. Security incidents in exclusively IT environments tend to result in extensive financial damage, but when it comes to vehicle security, it’s human lives that are on the line. This makes security the most important factor in connected vehicles, and security measures must be applied for safe communication between the car and the outside world.

Autonomous Driving

Autonomous cars frequently appear in popular sci-fi series and films depicting the future. Now in reality, autonomous driving technology is not a thing of the future but present reality. Many marine vessels and airplanes rely on autopilot technology to set automated trajectories for ships and aircrafts. The situation is more challenging with cars, however, as they must be able to adjust to changing traffic conditions, making autonomous technology for cars still a work in progress.

Companies across the world are making significant investments in R&D to develop autonomous technology for vehicles. At the same time, reports of self-driving cars being involved in fatal traffic accidents often make the news headlines.

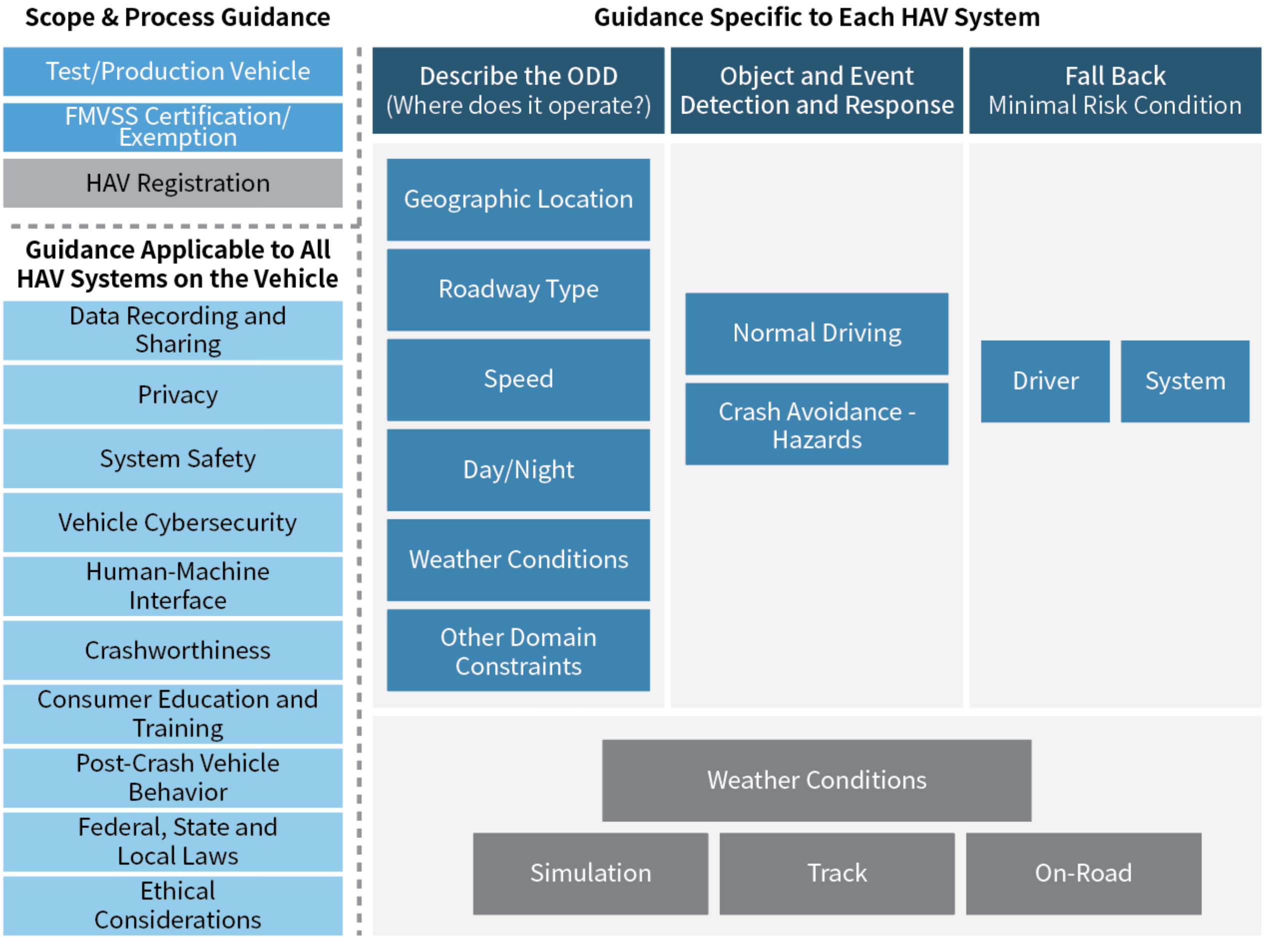
The levels of autonomous driving technology are defined in SAE International's standard J3016, which provides five different levels of automation ranging from 0 to 5. Vehicles in Level 3 and above are considered autonomous vehicles. Some firms claim to have developed driverless technology of Level 3, and some say they have made it up to Level 4.



Source : iQ.intel.com

However, does that mean Level 4 technology is more advanced than Level 3? The short answer: not necessarily.

Detailed guidance into developing autonomous driving technology is provided in the Federal Automated Vehicles Policy, published by the U.S. Department of Transportation and the National Highway Traffic Safety Administration (NHTSA) in 2016. According to the guidelines, engineers must define and document the Operational Design Domain (ODD) of an autonomous vehicle and make it available for review.


Scope & Process Guidance
Test/Production Vehicle
FMVSS Certification/ Exemption
HAV Registration
Guidance Applicable to All HAV Systems on the Vehicle
Data Recording and Sharing
Privacy
System Safety
Vehicle Cybersecurity
Human-Machine Interface
Crashworthiness
Consumer Education and Training
Post-Crash Vehicle Behavior
Federal, State and Local Laws
Ethical Considerations
Guidance Specific to Each HAV System
Describe the ODD (Where does it operate?)
Object and Event Detection and Response
Fall Back Minimal Risk Condition
Geographic Location
Roadway Type
Speed
Day/Night
Weather Conditions
Other Domain Constraints
Normal Driving
Crash Avoidance - Hazards
Driver
System
Weather Conditions
Simulation
Track
On-Road

Source : "Federal Automated Vehicles Policy", NHTSA, 2016

in which the autonomous vehicle is designed to operate. All ODD factors equal, a Level 3 vehicle may be considered more sophisticated than a Level 4 vehicle, but things get complicated when comparing two technologies with different ODDs. It's hard to say if a Level 4 vehicle cruising along the German Autobahn on a clear day is more technically capable than a Level 3 vehicle navigating a city center in pouring rain with extremely poor visibility.

In its guidebook, the NHTSA also proposes autonomous cars must comply with cybersecurity practices, but how is self-driving technology related to security?

Autonomous cars use a range of sensors, including cameras, radars, LiDAR and infrared sensors, to grasp the world around them and make immediate decisions on how to drive. Due to real-time sensor data analysis and decision-making technology still being in development stages, some attempts to operate autonomous cars have resulted in tragic accidents. In 2016, a Tesla driver was killed after the autopilot sensors on the car failed to distinguish a white tractor-trailer crossing the highway against a bright sky.[6] In this case, it would be possible for hackers to disrupt normal sensor operations or confuse sensors by feeding them misleading information to cause undesirable situations. Just like humans tend to experience poor vision when abruptly exposed to bright light, any camera attached to a car can temporarily lose sight of all objects around it, even if within close proximity, due to a drastic intensification of lighting. This kind of attack does not require sophisticated equipment or skills - it can be recreated using a powerful lamp, a massive mirror, or any other highly reflective surface.

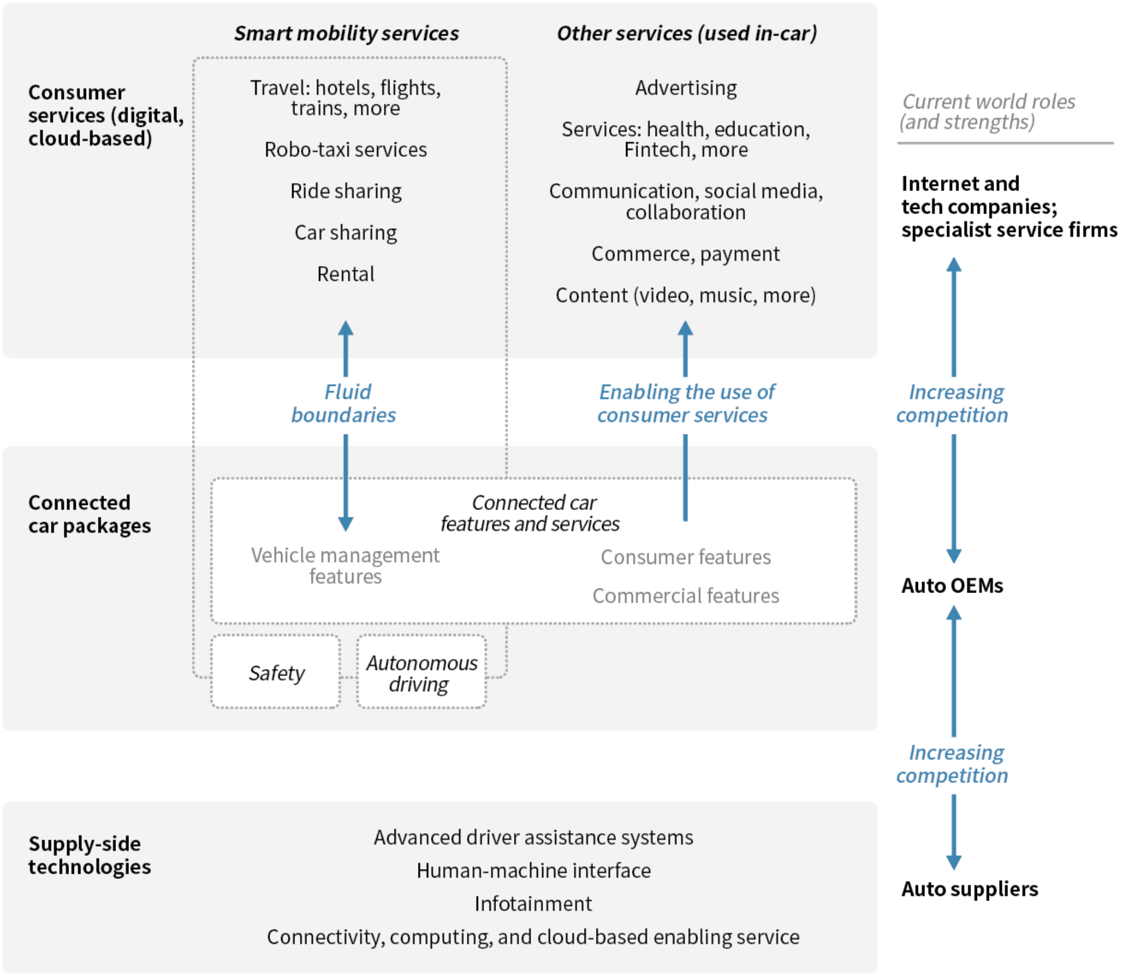
Due to internal sensors in cars providing only a limited range of information, autonomous cars utilize information shared by other vehicles and road infrastructure for responsible decision-making. This kind of self-driving technology is called cooperative autonomous driving. As previously explained in the Connectivity section, cooperative autonomous driving is built upon V2V and V2I communication. It’s important to note, however, that because information exchange is occurring via communication with external actors, all communication must take place only between verified trusted parties and channels.

Autonomous driving technology can also involve V2N or V2C communication to enable coordination at scale. Imagine a taxi company with a fleet of autonomous cars. When a customer calls the company to request a taxi, the company has to relay customer information to the designated taxi, and also be able to track its taxis in real time to allocate more taxis to any high-demand areas in advance. This coordination takes place with V2N or V2C communication. Security is therefore important in the field of autonomous driving which relies on and partakes in the movement of data between a multitude of external devices and servers for data processing.

[6] http://www.straitstimes.com/world/united-states/tesla-car-on-autopilot-crashes-killing-driver

Platform

With cars becoming increasingly connected, many companies are now eyeing business expansion via services designed specifically for connected cars. The conventional car business consists of two main markets: the car manufacturing market (vehicle equipment manufacturer and automobile manufacturer) and the aftermarket (vehicle part sales, car finance, and car insurance). However, with the emergence of connected car services, the entire car business industry is facing changes.


Smart mobility services
Other services (used in-car)
Consumer services (digital, cloud-based)
Travel: hotels, flights, trains, more
Robo-taxi services
Ride sharing
Car sharing
Rental
Advertising
Services: health, education, Fintech, more
Communication, social media, collaboration
Commerce, payment
Content (video, music, more)
Current world roles (and strengths)
Internet and tech companies; specialist service firms
Fluid boundaries
Enabling the use of consumer services
Increasing competition
Connected car packages
Connected car features and services
Vehicle management features
Consumer features
Commercial features
Auto OEMs
Safety
Autonomous driving
Increasing competition
Supply-side technologies
Advanced driver assistance systems
Human-machine interface
Infotainment
Connectivity, computing, and cloud-based enabling service
Auto suppliers

Source : pwc.com

One of the new emerging services is car sharing. Inspired by the SaaS (Software-as-a-Service) market where software is available on-demand, some industry experts have started dubbing car sharing services as the MaaS (Mobility-as-a-Service) market. Others may be more familiar with the pay as you drive (PAYD) model, which refers to a payment system that adjusts rates based on the distance covered. This model has made a breakthrough in the car finance industry, with numerous insurance companies now offering

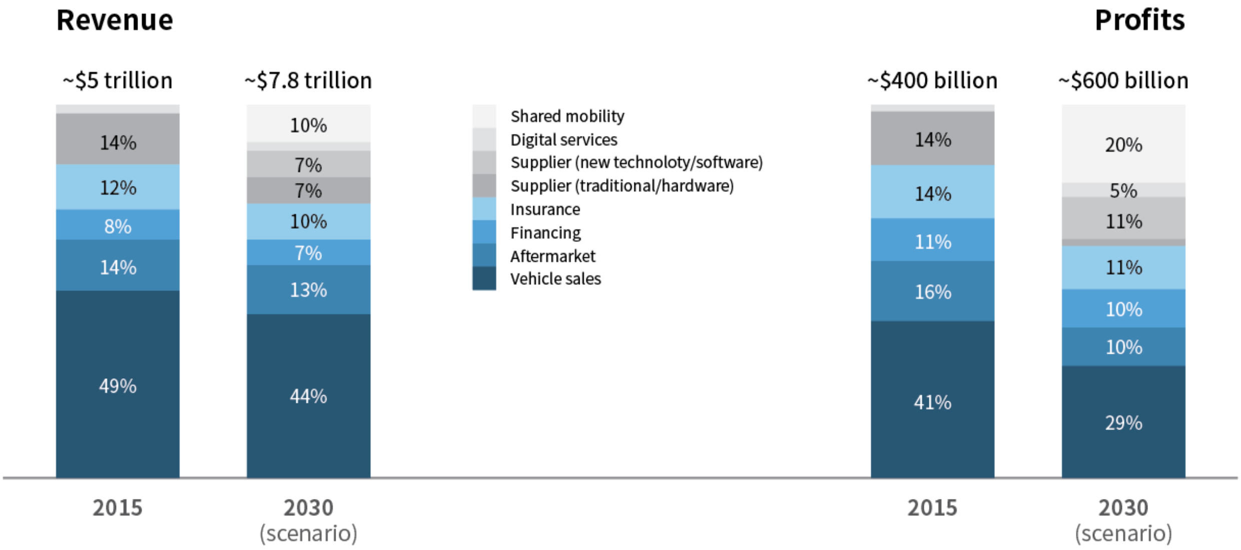
PAYD programs.

The transformation of mobile phones also deserves a closer look, specifically, how they have evolved from feature phones to smartphones. While feature phones had their limitations, they were capable of connecting to the Internet. Smartphones, however, took the extent and opportunities of Internet use to a whole other level. Whereas users could not personalize the software settings of feature phones, smartphones are designed to allow for application installation and removal, along with other personalized settings. The shift from connected cars to smart cars is expected to be similar to the advancement from feature phones to smartphones. The decision-making power on car software now shifts from the automobile manufacturer to the car owner, who can also leverage increased connectivity via the Internet to make further personalized adjustments.

The explosion of smartphones led to the creation of various service platforms and ecosystems, which have proven to generate new value for the market. With the release of iPhone, Apple launched App Store and iTunes Store to provide its customers with platforms for downloading software and multimedia content, as well as invite app developers and content providers to join its tight-knit ecosystem. For the fourth fiscal quarter of 2017, Apple announced a revenue of $52.6 billion, with an all-time high quarterly record of $8.5 billion from platform-driven services.[7]

Many are expecting a similar transformation to hit the automobile market. With cars, the sales focus is anticipated to shift from hardware parts and accessories to various services that make driving more convenient and pleasant. This is what Apple has pioneered by providing various services via designated platforms for a complete Apple experience, and to showcase the hardware features of its products, such as iPhone and iPad.

[7] https://www.macrumors.com/2017/11/02/earnings-4q-2017/



Source : pwc.com

Observing studies proposing revenue and profit estimates for the years 2015 and 2030, the markets for new technologies, suppliers of new technology and software, the digital service market, and the emerging market for shared mobility were estimated to have market revenues below 3%, with profits less than 4%, in 2015.[8] The numbers are expected to experience a drastic shift by 2030, when revenue is expected to hit 19% and profits 36%.

In June 2016, the transport ministers of all 28 European Union member states signed and announced the Declaration of Amsterdam, aimed at fostering cooperation in connected car and autonomous car technology and innovation.[9] The agenda is broadly categorized into eight shared objectives. One of them provides direction for use of data, and how data generated via use of connected and autonomous cars could be used create to public and private value-added services. In other words, it states car data can be collected and processed to provide users with new services. Guidelines for web service and in-vehicle resource access using HTTP-based web technology are defined in the standards ISO 20077 and ISO 20078 for Extended Vehicles (ExVe).

Some industry players are picturing new markets and services for automobiles, whereas others are creating standards for web-based vehicle resource access. Every time a new smartphone app is installed, permission to access and save data on a remote server must be granted. Most phone users are prone to click “Agree” without hesitation to gain access to the app. In the near future, the same pattern is expected to govern the way we use cars as well. Online service platforms for cars will begin collecting data and saving

[8] https://www.strategyand.pwc.com/reports/connected-car-2016-study

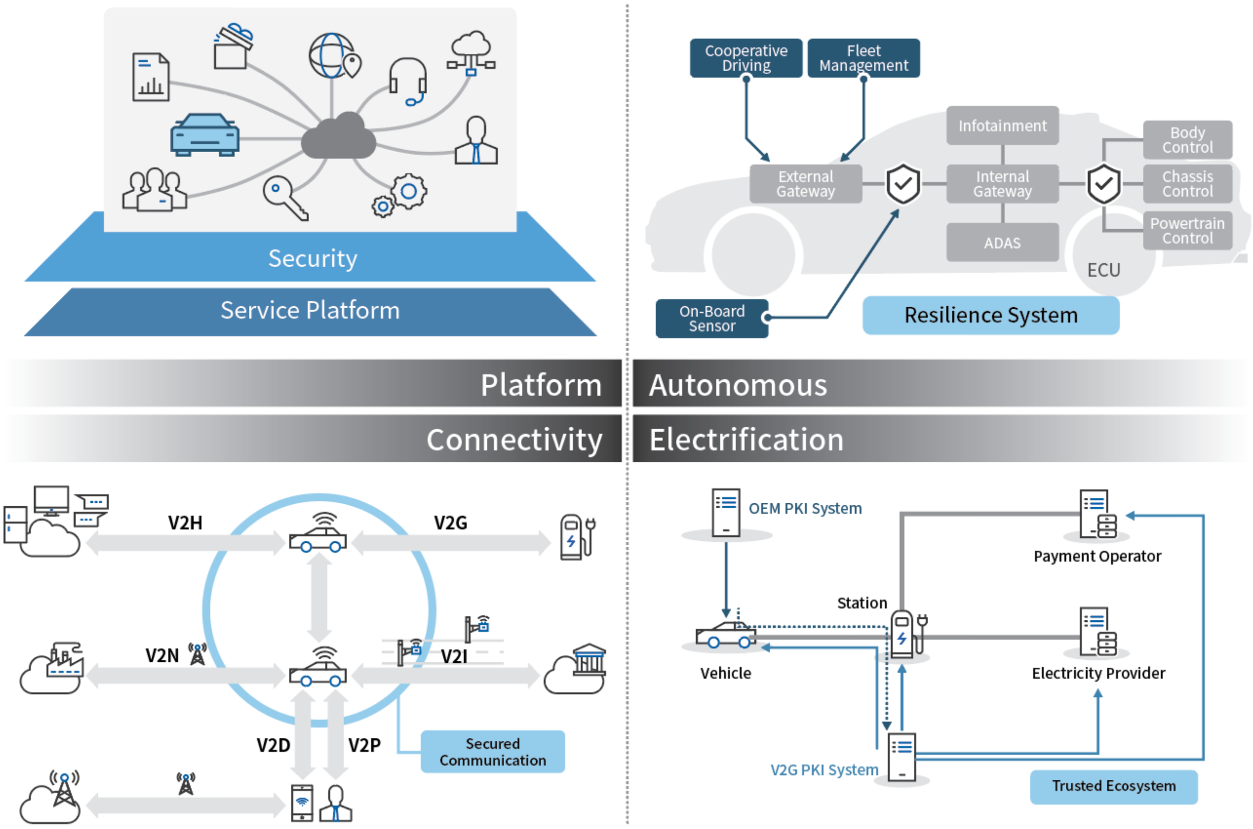
[9] https://english.eu2016.nl/documents/publications/2016/04/14/declaration-of-amsterdam

it on remote servers, and the same would be true the other way around, as cars will start retrieving data from online servers. Unlike traditional cars that were primarily modes of transportation, smart cars will become new spaces for online service consumption. Advancements in autonomous driving technology are allowing for increased driver freedom, and as drivers are no longer required to keep their hands on the wheel, the spare time freed up can be spent enjoying various online services. This is no different to how most people are spending their commutes on subways and buses glued to their smartphones.

While these new online services will emerge in response to advancements in car technology, the car will not be their central focus. To think about it, very few online services accessible via smartphones can be used with smartphones only. Instead, the services can be enjoyed using a selection of devices and a range of operating systems. Services and service platforms designed to connect with smart cars will become the main focus for business. Entering this framework will also be third party service providers, who will establish connectivity among the smart car, smartphones, and other devices. Much like Apple is leading change in the smartphone market with its ecosystem built around platforms, the smart car revolution is expected to be driven by platform-based services that form interactive ecosystems.

Security

Until now, we have taken a look into the changes brought about by PACE: Electrification, Connectivity, Autonomous, and Platform. Electrification, autonomous driving technology, and even platforms are all enabled by connectivity, which is key to changing the frameworks of external communication.



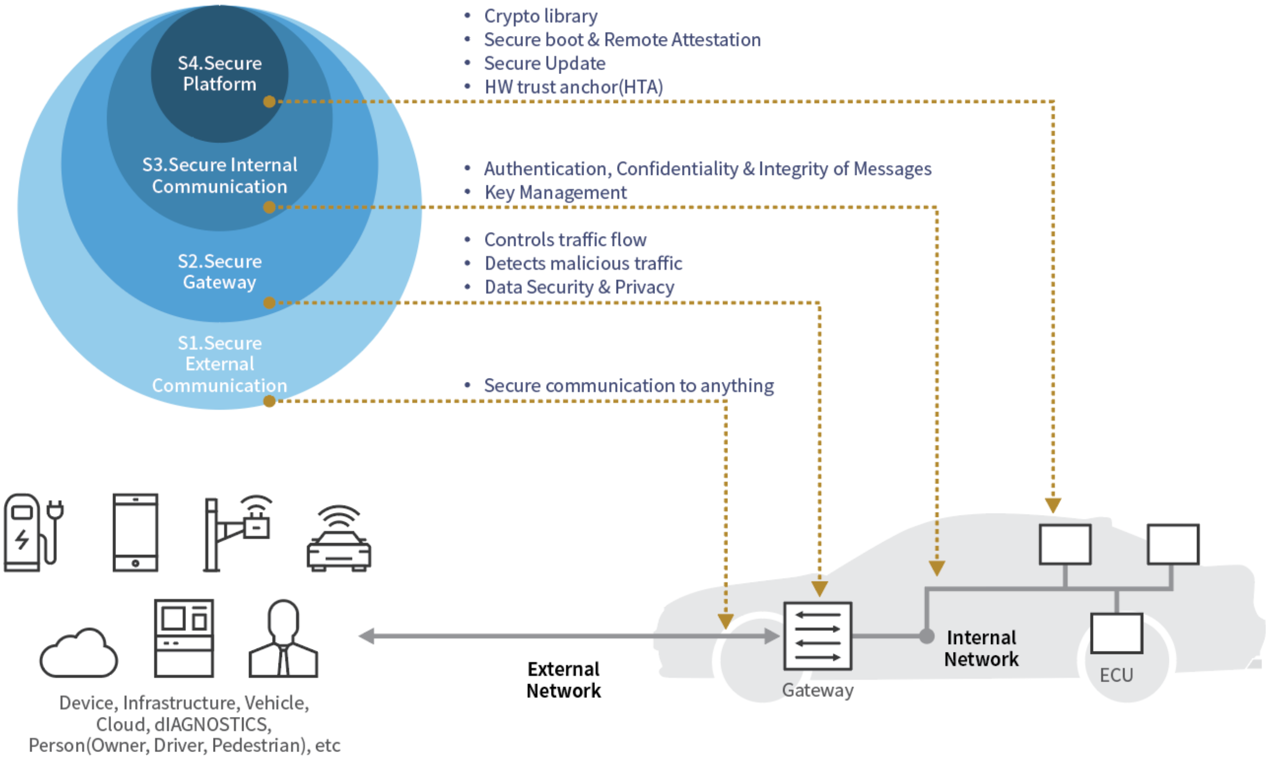
However, any communication model that connects the vehicle with surrounding actors or objects, such as V2V, V2I, V2P, V2D, V2H, V2G, and V2N, must be utilized only after establishing security over all communication. Without security in place, the vehicle can be exposed to potentially serious external threats. It's crucial to apply the principle of "Secure First, Then Connect" to vehicle communication, and always start with security.

In the electrification field, security must be applied to all communication between not only electric vehicles and charging equipment, but also any secondary actors involved in the exchange of electric vehicle data.

This is particularly important in securing the V2G communication model.

When it comes to online service platforms, everything revolves around the service itself, while cars, IoT devices, mobile gadgets, and other parties connect to not only the service, but also to other contributors in the service platform. Due to this interconnectivity, basic security measures such as authentication and encryption must be applied for secure operation of the platform.

In the case of autonomous cars, security must be applied due to external vehicle communication being directly linked to the car's ability to drive. Hence, authentication and encryption should be mandatory in order to secure all externally transmitted data. Even if the car does not engage in external communication, security must not be neglected. Unauthorized in-car controllers or malfunctioning controllers can interrupt normal system behavior in the car's internal network. It's also crucial to maintain stable and secure internal vehicle networks, and prevent injection of malware or attempts at other malicious attacks on the car. This can be solved via firewalls and intrusion detection solutions optimized for connected vehicles.


S4.Secure Platform
S3.Secure Internal Communication
S2.Secure Gateway
S1.Secure External Communication
• Crypto library
• Secure boot & Remote Attestation
• Secure Update
• HW trust anchor(HTA)
• Authentication, Confidentiality & Integrity of Messages
• Key Management
• Controls traffic flow
• Detects malicious traffic
• Data Security & Privacy
• Secure communication to anything
Device, Infrastructure, Vehicle, Cloud, dIAGNOSTICS, Person(Owner, Driver, Pedestrian), etc
External Network
Gateway
Internal Network
ECU

Vehicle security can be generally divided to the following four categories.

First is security technology for securing communication between vehicle and external parties or devices.

This allows for safe and stable operation of the car. Second involves measures that provide cohesive security for the car at the meeting point of external and internal networks. Those include intrusion detection technology that inspects traffic entering the car at the gateway level, firewalls that manage gateway routing, and data and privacy protection technology that allow for secure external sharing of internal car data. Third is security for internal vehicle networks. While cars are evolving into smart devices, they are still internally comprised of over 100 Electronic Control Units (ECUs) that connect to each other, forming an internal network. In order to secure communication among ECUs inside the car, security technologies like authentication and encryption must be applied to these networks. Fourth is security to ensure normal operation of all ECUs. This includes secure boot security that checks for faults during booting, remote attestation that analyzes the integrity of ECUs for remote entities, and secure update measures that provide firmware and software updates for ECUs. There's also the option of using hardware trust anchors (HTAs) that help secure ECU networks against hacking or tampering.

Some communication models for external vehicle communication, such as V2V, V2I, V2G, are already being secured using standardized security technologies. The problem is that other communication models lack agreed upon standards for security. The only solution is to foster cooperation among automobile manufacturers, car equipment providers, and security solution providers for a safer connected car future.

In conclusion, we have explored the five core elements that are driving revolution in the automotive industry. Only with a deeper investigation into how smartphones have transformed our society, can we begin to fully grasp the impact on our way of life that is to come with this changing mobility landscape. Conventional cars will become smart cars, and they are the next generation of smart devices to enter our lives.

The evolution of cars into smart cars will take time. But during that process, all parties from car owners to automobile manufacturers and government institutions must work together to create an efficient and valuable, but most importantly, secure environment for cars of the future.