CONNECTED CARS – ARCHITECTURE, CHALLENGES AND WAY FORWARD

Author: Dorairaj Vembu, Senior Product Manager & Evangelist, Automotive, Consumer Electronics & IoT

1. INTRODUCTION
The global automotive industry has been witnessing a transformation over the last decade with digital communication technologies making rapid inroads in vehicles. The world is moving towards the concept of connected transportation that focuses on providing enhanced connectivity like vehicles communicating with each other to know their presence, real-time communication facility to the occupants of the vehicle. This functionality is enabled by variety of technologies like vehicle to vehicle communication, vehicle to infrastructure, vehicle telematics, vehicle informatics that provide various services such as real-time street updates, smart routing and tracking, roadside assistance in case of accidents, automatic toll transactions, automatic parking/parking management, on-board entertainment, and much more.

1.1. GLOBAL CONNECTED CAR MARKET
The global connected car market is estimated to grow from $46.9 billion in 2015 to $140.9 billion in 2021. Safety and autonomous driving are the largest categories, accounting for about 61% of the total market. In the premium automobile segment, the spending on digital technology is expected to rise to 10% of total vehicle sales by 2021, more than double the current level of 4%.

OEMs and Tier-1s suppliers are making the related R&D investments. The volume segment of cars made for middle-income purchasers also sees auto makers adding basic connectivity functions. Here, digital content is on course to reach 2.6% of total selling prices by 2021, up from just 0.5% in 2015.
Globally, electronic components are expected to be 50% of the value of a car by 2030, from the current 30%. Considering that the volume growth in emerging markets will be in Low-Mid to Mid-High segments, the key to driving adoption in these segments is by arriving at electronics architecture that optimize on the costs while providing value to the customer.

This paper discusses the need for relevant and economic solutions, emerging trends and accompanying challenges that arise with growing complexity and evaluates the best-possible mechanism to overcome these challenges.

The paper also delves into the various components that get into the telematics control unit/wireless gateway beginning with analysis of the software components, complexities of a modern telematics system and optimization possibilities. It concludes with a view on the existing supply chain precision and the way forward.

2. AUTOMOTIVE ELECTRONICS ARCHITECTURE

Traditionally the Automotive architecture comprised of Infotainment, Telematics, and Diagnostics which acted as silos with minimal/no communication between them. The advent of advanced communication technologies like LTE, V2X has resulted in these silos being broken resulting in more seamless exchange of information across them. This has resulted in interesting use cases like Connected Infotainment, Real-time diagnostics and real time tracking.

Modern connected cars bring together various silos of an Automotive like Infotainment, Telematics, and Diagnostics through real-time communication systems enabling use cases that greatly enhance the user experience.
The software architecture of modern connected cars comprise of three main components:

- Connected Car Gateway (CCG) which forms the entry point for a car to communicate to external world
- Cloud based servers that perform real-time analytics on the data that is generated from the car generating real-time insights
- Applications on smartphone that provide an intuitive user interface that allow an user to interact with the car over wireless networks to perform variety of operations starting from getting vehicle status to controlling some of the aspects of the car like Switching on the HVAC or locating a car in the parking lot.
As seen from the architecture diagram above, newer Telematics systems are getting complex as features additions are on the rise. Traditional telematics units comprised of basic features like emergency calling, crash notification and basic 2G connectivity.

In contrast, Modern Connected Car Gateway unit comprises of advanced features like 4G connectivity, hotspot, cloud connectivity, vehicle to vehicle communication, ability to control the car remotely, Firmware update over the air (OTA), remote diagnostics, predictive maintenance apart from traditional features like eCALL, crash notification.

### 2.1 DESCRIPTION OF FUNCTIONAL BLOCKS

#### 2.1.1 OPERATING SYSTEM LAYER

Operating systems provide key functionality like scheduling, memory management, threading, application security, drivers to access the peripheral devices that can be used by applications.

While there are many operating systems available in the market like Linux, QNX, Android, VxWorks, the auto industry has been traditionally dominated by OS like QNX due to its reliability.
In recent times there has been a movement towards Linux due to costs, availability of talent to perform upgrade or maintain the system. Consortia like GENIVI, AGL which includes representatives from Automotive OEMs, Automotive Tier1s, and Silicon vendors are actively working towards creating distribution that contain automotive specific features that can be used by the industry. These distributions standardize the non-differentiating middleware allowing Automotive OEMs to innovate and add differentiating features on top of the middleware thus reducing the costs and enabling lower Time to Market.

Android based systems are making their entry into IVI systems mainly due to ability to re-use the applications developed for Mobiles/tablets in the IVI systems. The uptake of Android has not been spectacular in Auto industry as against mobile industry since each OEM would want to provide his own custom user experience/brand experience against nearly uninform experience provided by Android. The frequent Android updates, the perception of not being able to meet the reliability requirements of Auto Industry, Open Source issues, inability of the OEMs to influence the roadmap add to the problem.

2.1.2 VIRTUALIZATION LAYER

In order to optimize on the hardware costs, the Connected Car Gateway market is seeing a phenomenon of ECU consolidation where multiple functions like IVI, Connected Car Gateway, and Digital instrument cluster are integrated into a single ECU. The key challenge is that the reliability requirements of each of these systems are different and fault in any one system should not affect the other. Adding to the challenge is the fact that Tier1s have developed and matured these systems over the years and would like to re-use these assets.

Virtualization provides an option to share the hardware resources across multiple applications running across multiple OS. Virtualization can be achieved by use of hypervisor on top of hardware.

There are various hypervisors in market classified mainly as Type 1, Type 2 hypervisor. Each has its own benefits and choice of type of hypervisor is mainly dictated by the type of applications that are can to run on these systems.

Type 1

Under Type 1 hypervisor the following options can be considered:

Full Virtualization

Full virtualized system provides complete hardware abstraction to the OS above creating a view to the OS that each one has its own hardware. Thus multiple guest OS can run on the hypervisor without any modification. Issues in one Guest OS do not affect the other.
Para Virtualized System

Para virtualized systems are those that try to remove the overhead associated with binary translation involved in Type1 hypervisor. This in turn provides better performance than type1 hypervisors since the OS and hardware are knit more tightly. This is crucial for operations that are IO intensive, compute intensive like graphics, multimedia, gaming engines etc. In para virtualized systems, the privileged access to hardware is provided by what is called a Dom0 system that:

- Acts as a server to its para virtualized clients
- Directly access the hardware functionality

In terms of the available choices, proprietary hypervisors available in the market are:

- Green Hills Integrity
- Open Synergy’s PikeOS
- QNX’s Hypervisor
- Open source options include Zen hypervisor

Type 2

In Type 2 hypervisors, one has an OS like Linux, running on top of bare metal and running a hypervisor in the Linux OS. Multiple guest OS run on top of the type 2 hypervisor. Due to multiple level of indirections involved, such systems provide degraded performance as compared to Type 1 hypervisor. The advantage of the system is that if there a Linux port available for the hardware, a virtualizer can be run on the Linux OS and guest OS can be easily configured.

2.1.3 CONNECTIVITY

Connectivity block is a very important block of a CCG. It comprises of various blocks like Long range connectivity modems like LTE, Short range connectivity modems like Wi-Fi, and BT positional tracking systems like GPS.

- Modem connectivity

Modem connectivity is required for transmission and reception of data in real-time to/from internet. At the lower end we have 2G/2.5G modems which provide data rates less than 100kbps going to LTE which provide data rates at few Mbps. Modem integration can be done using either dedicated modules from vendors like Telit, Sierra wireless or using inbuilt modem that comes as part of SOC delivered by vendors like Qualcomm.

- eCall

eCall services provide emergency alerts to the Public Safety Access Points in case of emergencies so that help can be provided to the victims at shortest span of time. In most cases it involves communicating information about the accident including location, number of occupants, speed, direction etc. (Vehicle Emergency Data Set) that can help the recipient of the information to assess the severity of the incident and provision necessary help. eCall service is built on top of the modem.
The EU has passed a regulation that requires all passenger cars to be equipped with eCall systems by April 2018. The regulation was passed on April 28, 2015. For example, the eCall technology works in such a way that in the event of a serious accident, the system automatically dials Europe’s emergency number – 112.

The Global standards for eCall is emerging with 3GPP standardizing the eCall requirements as part of 3GPP TS 26.267, TS 26.268. The transmission of VEDS is followed by an automatic call to the call centre so that a voice communication can be established with the occupants of the car.

In the U.S., the Net GEN 9-1-1 envisages to enable a Public Safety Answering Point to automatically receive and process the VEDS (Vehicle Emergency Data Sets). USA is yet to adapt a standard protocol for eCall though some of the telematics services providers in USA like GM OnStar, Ford Sync's 911 assist, Lexus Link etc. provide similar services and each one of them use their own proprietary method for transmitting data to the call center.

2.1.4 V2X

V2X technologies help in real time communication between vehicle to vehicle and Vehicle to infrastructure so that a vehicle is aware of the environment around it thereby avoiding collisions with other vehicles.

Traditionally V2X is based on 802.11p technology. This technology is based on 802.11a (5.8GHz band) with increased range at cost of lower bit rate and 802.11e for QoS. QoS helps in priorities the messages and further reducing the delay.

A new technology based on the LTE standard called LTE-V is also competing for usage in V2X communications. This technology is trying to standardize long range as well as short range communication system. LTE infrastructure synchronizes the stations for point-to-point communication as well, which enables better data throughput, Packet Delivery Rate (PDR) and offers lesser end-to-end delay than 802.11p based technologies.

2.1.5 FOTA

With software content in Connected Car Gateway unit increasing by the day and considering that the average telematics unit has a life span of over 7 years, it is natural that the unit needs software updates periodically. Software updates are also needed to fix the issues that appear during the field run including security vulnerabilities that are un-covered from time to time. FOTA (Firmware Update Over The Air) module helps keep the software in Telematics up to date.

According to a new report by ABI Research by 2022, there will be 203 million vehicles on the road that can receive over-the-air (OTA) upgrades; among these vehicles, at least 22 million will also be eligible to get firmware upgrades. Research expects the sales volume for consumer vehicles to be approximately 625 million units between 2016 and 2022. So, the percentage of OTA-enabled vehicles across the 2016-2022 timeframe would be 32% of the total sold.

2.1.6 SECURITY

The security module implements various mechanisms to secure the telematics control unit from malicious code. This involves
mechanisms like Secure boot, secure storage for storing the keys, Secure communication with external world like SSL, TLS, Application signing, Access restriction/privilege control to for various types of applications to access system peripherals, vehicle bus like CAN.

### 2.1.7 APPLICATION FRAMEWORK

Connected Car Gateway Application framework implements a SDK that allows 3rd parties to develop applications that can be downloaded into the device. This will enable development of an ecosystem to provide variety of services using the data that is available from Connected Car Gateway box like Usage based insurance, preventive diagnostics, location based services

The framework abstracts all hardware specific intricacies from app developer. The framework exposes APIs in Java/HTLM5/JS allowing ease of programming

### 3. CHALLENGES IN DEVELOPMENT OF CONNECTED CAR GATEWAY

#### 3.1 COST OPTIMIZATION

Mass penetration of Connected Car units is required to ensure that the participants benefit from the network effect. E.g. a V2X solution integrated in majority of the vehicles ensures that these vehicles exchange information about their location, speed and there by prevent accidents. This requires that the telematics unit be available at attractive price points for mass market adoption. This puts pressure in terms of optimizing the hardware cost, Software costs and associated maintenance.

### 3.2 COMPLEXITY

The Connected Car systems are getting complex due to

- Integration of Multiple connectivity technologies like 3G, LTE, Wi-Fi, BT and need to seamlessly interop with the network operators
  - These are the areas that are new to automotive industry and traditionally been the forte of players in telecom industry
- Broader ecosystem
  - As the complexity of telematics systems have been increasing with more functions getting integrated in to the system, the ecosystem has widened. Today’s ecosystem comprises of players like TSPs, Application framework providers, Providers of various types of software like FOTA, Telematics middleware, Telematics app developers, Telematics service providers. This has resulted in requirements for Connected Car solutions to be open enough to be able to add new apps/services to be in tune with changing needs of market while at the same time be safe and robust enough not to compromise on safety/security

#### 3.3 RACE TO KEEP PACE WITH TECHNOLOGY

The mobile/consumer electronics industry has seen rapid advances in the past couple of years.
Lot of new features/services figure as a part of these rapid advancements and there has been tremendous pressure on the automotive industry to keep pace with these changes and cater to the growing demand of offering the same features or more to its customers. The key challenge that the automotive industry has in keeping pace with the rapid changes is its long product cycle, quality requirements and validation cycles. Typically consumer electronics/mobile industry can quickly incorporate new feature/services and move on to the next big thing if it is not successful but the same is challenging in automotive industry.

3.4 SECURITY

With more and more vehicles getting connected to network today, the possibility of an intruder getting access to internal vehicle network and performing malicious activity are real threats.

The infamous Jeep hack was that someone was able to physically compromise a car since it was engineered in the old school of technology. Any failure at one single point would result in breakdown of cryptographic chain of trust. The Connected Car units that are connected to internet need to implement multiple layers of security so that break in one layer does not compromise the entire system. The software security issues has to be addressed at various levels right from the time the firmware is flashed in factory, going all the way to ensuring integrity of downloaded applications and workshops where the firmware will be flashed.

4. INSIGHTS AND PERSPECTIVES ON THE SOLUTION TO THE CHALLENGES

4.1 APPROACHES FOR OPTIMIZATION OF COSTS

The following approaches are considered for optimizing the costs of Connected Car Gateway:

- Consolidating multiple functions into a single SOC/Hardware block using Virtualization
- Choice of OS (use of Open Source OS)
- Consolidate connectivity blocks
  - Use a SOC that integrates various connectivity blocks like LTE, Wi-Fi, BT, and GPS. A pre-validated modem with necessary software from chipset vendor would greatly contribute towards reducing the development costs

4.1.1 CHOICE OF VIRTUALIZATION METHOD/HYPERVISOR

The choice of type of hypervisor and OS depends on the type of applications that will be run on the system.

A system where existing applications have been developed on different OS and each of these applications do not perform compute intensive operations like Graphics, Multimedia, can benefit by use of the Type 1 hypervisor. The reliability and maturity of the applications that have been ported can be carried forward while
saving on the hardware costs by sharing the hardware.

For systems that need to perform compute intensive functions like Multimedia, Graphics from an OS like Android while running traditional functions from OS like QNX, Linux, a para-virtualized system can be considered. In this case the Android system can make use of the traditional hypervisor functions for functionality like Memory, File system, and scheduling while it gets the benefit of hardware accelerated graphics, Multimedia through the para virtualization

4.1.2 CHOICE OF OS

Operating System forms the layer that sits above the hypervisor and is a key component of any Connected Car Gateway.

While the basic requirements for choice of OS depends on need of near-real time scheduling capabilities, reliability, foot print, availability of base port in popular SOC some of the other key considerations are:

- Cost (Licensing fee, Royalties etc.)
- Maintainability/Upgradability/Scalability – Access to source code, availability of talent to work on updates, adding support to new peripherals

4.1.2.1 KEY ENHANCEMENTS REQUIRED IN LINUX FROM AUTOMOTIVE PERSPECTIVE

- Fast boot to enable early access to certain peripherals
- Secure boot
- Power optimization:
  - The Connected Car Gateway needs to optimize power under sleep mode (To be able to wake up to commands from remote location when left un-used for long time). The Connected Car Gateway will be running on battery power and hence the need to optimize power consumption
  - Reliability/Fault tolerance

The Tier-1 can adapt Linux to address these needs by adding its own ‘customizations’/ ‘Secret Sauce’ to the Linux distribution provided by the open source community. In this way, while one can benefit from the updates provided by the open source community, the differentiation can be achieved by vendors own customizations.

Low end systems that are focused on very specific tasks would benefit from using an OS with low memory foot prints. Examples of such cases are entry level infotainment systems, telematics systems. Various commercial RTOS available in the market are the possible choices.

High end infotainment systems, Connected Car Gateway would benefit from OS like Linux/Android due to their cost, support for various chipsets, large ecosystems.

4.2 CONNECTIVITY INTEGRATION

4.2.1. SELECTION OF CONNECTIVITY MODULE

Traditionally every device manufacturer takes a module from module provider and integrates into the system. These modules provide the benefit of ease of integration and Time to market by:
• Providing simple software interfaces like AT commands
• Taking care of interference issues when multiple connectivity technologies are coming together like Wi-Fi, BT, interference of operating frequency bands
• Certification and compliance

However these modules have a drawback in terms of having higher cost and do not justify the cost-volume economics at higher volumes. These modules have been traditionally used in CE markets and adapting these to automotive market poses challenges as the reliability requirements of these markets are different. The subsequent sections address some of the key requirements/consideration in integrating connectivity module in Connected Car Gateway.

**HOW TO SELECT THE CONNECTIVITY BLOCK**

From the perspective of optimizing the costs and reducing the TTM, the following approaches may be followed:

**High volume product:**

Take an integrated SOC comprising of application processor and all connectivity blocks and add specialized components like GPS in case the component provided by SOC does not meet the required specification.

**Low volume product:**

Take discrete connectivity modules that are proven in the market and integrate them together. The unit costs would be higher but the lower NRE and Time to market advantage would compensate the higher unit costs

**4.2.2 MODEM INTEGRATION**

Modem integration for a Connected Car Gateway in automotive is different from integration of modem into a mobile phone and has its own complexities. Additional considerations have to be done in following areas:

**HARDWARE PERSPECTIVE**

- Roof Mount Antenna:
  - This could cause a gain in Downlink but 3GPP power restrictions in uplink causes device failure in uplink.
  - False indications due to additional antenna gain, leads to miscalculation of handover border by the network.
  - Issue related to VoLTE, SRVCC due to uneven gain in downlink

- Internal antenna
  - Additional interference due to car body metal and at times there will be lower RF penetrations. These causes download speed issues. Interference issue becomes more severe as different vehicle have different material, design, curvature which means that means that antenna gain/interference keeps changing vehicle to vehicle

- Location services
  - For GPS, the traditional accuracy provided by general purpose module that integrates LTE, Wi-Fi, BT, GPS do not meet the needs of automotive use cases like ADAS/V2X that require accuracy of 1 meter

**SOFTWARE PERSPECTIVE**
The following issues need to be addressed from Software perspective:

- **Handover and Fall back**
  - Seamless handover from one radio to another radio (4G to 3G/2G) and across multiple operators has to be implemented and tested to ensure that there is continuity of services. This is very critical from provisioning of emergency services.

- **IoP and compliance**
  - The solution needs to interoperate with equipment deployed by various network operators/roadside infrastructure operators. This requires extensive field trials across the country with varying terrains from red-hot deserts to freezing mountains. In addition the solution needs to be compliant with the 3gpp, V2X and other specifications published by standard bodies.

- **Moving from Mobile standards quality to Auto standards**
  - The solution deployed in automotive environment needs much rigorous testing compared to those deployed in mobile industry to meet reliability requirements of auto industry. The complex interplay of hardware + software issues at tiring environmental conditions (e.g. Signal reception failing when temperature increases beyond a particular threshold) require special attention.

4.2.3 SERVICES INTEGRATION – eCALL

The key challenges in implementation of eCALL services include provision to try out all possible means to communicate the information about the incident so that help is made available. These include:

- Evaluating various bearers available for transmission of the VEDS and establishing a voice call and selecting the best connection.
- SIM provisioning in a way where roaming to other carriers are allowed.
- Redundancy in transmission of VEDS over different networks including SMS if packet data connection failed.
- Automatic retries.

4.2.4 NEW TECHNOLOGIES – V2X

V2X technologies enable real-time communication between Vehicle to Vehicle and Vehicle to roadside infrastructure. Over the years 802.11p has evolved as an option for enabling V2X communications and there have been trials around the globe to demonstrate feasibility of 802.11p for V2X communications. In recent times, the 3gpp consortium has come up with LTE-V as an alternative for 802.11p.

When one compares both these technologies, the behaviour of both these technologies varies when the number of stations increases. Speed of vehicle has effect in PDR and end-to-end delay. LTE-V outperforms 802.11 based technologies in both the cases, but has limitation that its standardization is still in progress. So adaption of this technology will delay in commercializing the product. On the other hand 802.11p is infrastructure-less technology, so easy to build a commercial product.
Both these technologies can benefit from the higher layers (L3 and Above) in terms of re-use of the higher layer standards like WSMP protocol for transmitting control information, traditional IP stack for convenience services, IEEE 1609.1, IEEE 1609.2 for security and remote management services.

In terms of compute requirements, the base band (L1 and L2) requires use of a processor with real time processing capabilities running RTOS like VxWorks or equivalent. With respect to the choice of where the protocols starting at L3 need to run, it depends on the use case. Use cases related to Imminent Collision Warning, Adaptive Cruise control... require real time performance and strict latencies. These kinds of applications would require protocols like WSMP and higher layer applications to run concurrently on the same processor where the MAC is implemented.

For use cases where there are no strict latencies like Access control, Virtual Gantry, Applications related to different notifications like road condition warning, work zone warning... both these technologies (802.11p and LTE-V) can run on same application processor as that of a Wireless gateway with the dedicated Wireless module for LET-V/802.11p providing the PHY and MAC layer services.

### 4.3 FOTA

The key challenges in FOTA integration are:

#### 4.3.1 SOFTWARE DISTRIBUTION

The distribution of software update can be done by setting up a dedicated server that distributes the software to various locations of the servers to take care of large scale updates; similar to that of Content Delivery Networks

#### 4.3.2. FAIL SAFE & RECOVERY

Challenge here is to ensure a backup image in place in case there is a failure of update due to reasons ranging from link loss to loss of power.

#### 4.3.3. OPTIMIZATION OF BANDWIDTH

While a Connected Car Gateway image can run into hundreds of MBs, it is necessary to ensure that the FOTA updates are optimized to conserve the bandwidth by segmenting the image into various logical groupings and ensuring that only the required part is updated instead of the whole image (Delta updates)

#### 4.3.4. SOFTWARE INTEGRITY

It is necessary to ensure integrity and genuineness of source of the image that is being updated. This can be achieved by fusing the security keys for CCG at the time of production and validating it in real-time during activation. Asymmetric and Symmetric cryptographic functions along with Hash of images can be used to ensure that the image is secure while ensuring that the time spent on decrypting the image during boot is kept minimal.

Updates of ECU software require special care and consideration. Many of the ECUs are based on low power processors that cannot perform heavy cryptographic functions.

The possible solutions could be to have an ECU gateway run a powerful processor that decrypts the image and distributes the images to various ECUs connected to the gateway. Redundancy
has to be built in at the gateway level to ensure that there is another CPU to take over in case of failure.

4.4. VEHICLE NETWORK SECURITY

With more and more vehicles getting connected to internet allowing access to vehicle information and control of vehicle from remote location, the security threat to vehicles from external hackers has increased exponentially.

While there is always a possibility of using powerful CPU and implementing strong crypto function, there is a trade-off between cost and performance one has to make. Traditionally Vehicle networks are based on low power microcontrollers and they don’t have much processing capability to do heavy crypto algorithms. The capability of hackers is increasing much faster than the hardware systems capability.

In the rapidly changing scenario where new issues are un-covered on daily basis, vehicle security has to be looked at from systemic perspective. Legacy Vehicle networks are based on low power microcontrollers and these microcontrollers do not have high processing capability for heavy crypto algorithms. The capability of hackers is increasing much faster than the hardware systems capability. Thus any type of crypto processing at end nodes is not recommended. The crypto/security issues need to be captured at the gateway/entry point.

With multiple layers of security, isolation of vehicle interface networks from external world etc. Some of the solutions include

- Isolation of systems in the CCG (IVI vs Vehicle Interface Network)
- Intrusion detection prevention systems which monitors suspicious activity on vehicle network and provide alerts
- Secure communication with external world using protocols like SSL/TLS
- Software based access control mechanism (like ACL) for 3rd party applications by restricting access to Automotive Message brokers.
- Having a powerful gateway that can have exclusive access to vehicle network. The gateway can perform heavy crypto processing and validate the software that goes into the ECU

4.5. APPLICATION FRAMEWORK

The Application framework should provide a SDK that is simple enough to abstract all the hardware intricacies from application developer yet be secure enough to prevent un-authorized access to the underlying vehicle network. The framework has to implement APIs that allows ‘signed/trusted’ applications access to privileged data/peripherals and standard API that can be used by regular developers.

The Connected Car ecosystem has seen emergence of Multiple Telematics Service Providers with each of these TSPs using its own proprietary methods/protocols to exchange data with the CCG. The framework has to provide hooks to integrate implementations from various TSP or better API layer that needs to be ported as one moves from one TSP to another. This has the benefit of re-use of the applications written across multiple TSPs by porting the TSP specific layer
Typical choice for framework include J2ME based framework that allows Java Apps to be run on the CCG or HTML5 framework that allows applications to be run from HTML5 browser.

5. WHERE IS THE TELEMATICS INDUSTRY HEADED TO?

5.1. RICHER FUNCTIONALITY AND INCREASED COMPLEXITY OF CONNECTED CAR GATEWAY

- Connectivity hub in a Car with wide range of connectivity technologies like Wi-Fi, LTE, NFC, BT
- Telematics box could be potentially a hub for some of the ADAS features using LTE Direct that provides low latency P2P communication using priority messages/alarm messages, complementing the 802.11p
- Open Connected Car platform is the future where tier1s provide a platform and expose an SDK where 3rd parties can develop a variety of apps and provide the services

5.2. INNOVATIVE BUSINESS MODELS FOR DATA MONETIZATION WILL EMERGE

While the user owns the data, he is not able to monetize the same. So 3rd party TSP/Brokers will emerge who will get into an agreement with users to trade the data for useful services. The 3rd party TSP can make this data available to app developers that can be used for variety of purposes

5.3. SECURITY WILL BE A MOVING TARGET BUT LEVELS OF SECURITY WILL INCREASE RESULTING IN HIGHER ADOPTION

This is a concern and has to be addressed at systematic level. Standards have to emerge right from accessing that data securely from vehicle network, to transmission to cloud, protecting data in the cloud. Some sort of certification levels establishing a common baseline has to emerge. This information has to be published so that a user is aware of how secure the car is. This requires coming together of TSP, Tier-1s, Auto manufacturers, App developers. The security promise will help prospective car buyers to embrace the connected car philosophy with more ease.

6. CONCLUSION

Connected Car technology is here to stay. The success depends on adaption and emergence of business models that would allow constituents to earn revenue. The Technology provides opportunities for new ecosystem players like providers of Components, On-board software, wireless connectivity, delivery infrastructure, telematics service, Infotainment content, Application developers to enter the market and bring in innovative areas ideas from non-automotive domains.

The industry has already seen emergence of interesting use cases like Autonomous Cars, Car Sharing that has resulted people moving away from owning cars to ‘Summon a ride’ or Usage
Based insurance where users pay for insurance based on their usage and driving habits.

It is clear from the discussion in this paper that there are enormous technological challenges in developing the Connected Car Solution which requires collaboration between people from various industries like Telecommunication, Automotive, and Computer/Software. The situation is similar to the early days of the mobile industry when there were no uniform standards for development of services/application on devices resulting in a fragmented eco-system.

While the communication aspects of connected car technologies are standardized owning to their origins from the mobile industry, the service related aspects need to be standardized.

The coming years would see standardization and possibly growth of these functions leading to a vibrant ecosystem of connected car application/services developers and successful business case. Soon the car will not just be a ride to go from one place to another but would rather be an experience travelling from one place to next.

7. ABOUT THE AUTHOR
Dorairaj Vembu spearheads the technology led business development addressing Automotive Electronics and the Internet of Things. He has rich experience in Product Management, product development, program management in Infotainment, Multimedia, Connectivity and the Consumer Electronics space. He has worked on product definition and created roadmap to help global Tier-1 vendors launch first-to-market products and manage the Product Development Lifecycle. He has also helped put together process and systems to develop and manage an ecosystem of partners for the co-creation of products. During his career spanning over 19 years, Dorairaj has held various engineering positions starting as a developer and graduating to a solutions architect. He has been instrumental in harnessing Sasken’s key strengths in Telecommunication, Multimedia to successfully penetrate and entrench Sasken as a key player in the Automotive Electronics and Consumer Electronics space. His interests lie in Connected Cars, its evolution and future, usage based insurance and smart cities. He also has the responsibility of being Sasken’s evangelist for the Auto and IoT business and has spoken at several industry forums and published articles in leading magazines. He has authored and co-authored articles that cover improvement of urban governance by leveraging the smart city concept. Dorairaj has a Bachelor’s degree in Computer Science from NIT Trichy and an MBA from IIM Bangalore.

8. ABOUT SASKEN
Sasken is a leader in providing Product Engineering services and Digital IT services to global tier-1 customers. Sasken’s deep domain knowledge and comprehensive suite of services have helped global leaders maintain market leadership in Semiconductor, Automotive, Telecom, Consumer Electronics, Retail, and Automation.

Address: Sasken Communication Technologies Limited, 139/25, Ring Road, Domlur, Amarjyoti Layout, Bengaluru, Karnataka – 560071, India.

© Sasken Communication Technologies Pvt. Ltd., 2016

www.sasken.com

Date June 30, 2016