Chapter 1
An Overview of Automotive Vehicles and Information Security

Madhusudan Singh

Abstract In this chapter, we present the International SAE (Society of Automotive Engineer) six level development of vehicle automation and their information security challenges. In addition, we have introduced the history of automotive technology revolution and discussed about vehicles development stages. We have discussed threats of advanced automotive technologies such as self-driving car and its components. Finally, we discuss several automotive technologies with the association of information technologies.

Keywords Intelligent vehicle · Autonomous vehicles · Information security

1.1 Introduction

The evolution of the automotive industry began in the 1890s. Now at the dawn of the twenty-first century, this industry is over 130 years old. The automotive industry is an industry characterized by a safety culture that became systemic in the 1960s. This industry is characterized by tremendous growth as the number of passenger cars alone are estimated at about one billion. Future projections are even more expansive. Unlike the automotive industry, the information technology industry started with the propagation of computers and information technology systems (IT systems) as early as the 1950s. This created a usage explosion in the 1990s that led to todays wired environment. Although this industry is only 70 years old, the processing power increased exponentially. With the combination of wireless internet and with location finding capabilities, the IT industry has created a new paradigm for human existence. The Information Technology Industry is characterized overall by a security driven culture: this stems from the fact that IT focuses on data, which analyzes trends and models [1]. In recent times, there has been an ever-increasing merging of the automotive industry with the information technology industry. Everyday vehicles utilize an

M. Singh (✉)
School of Technology Studies, Endicott College of International Studies, Woosong University, Daejeon, Republic of Korea
e-mail: msingh@wsu.ac.kr

M. Singh, *Information Security of Intelligent Vehicles Communication*,
Studies in Computational Intelligence 978,
https://doi.org/10.1007/978-981-16-2217-5_1

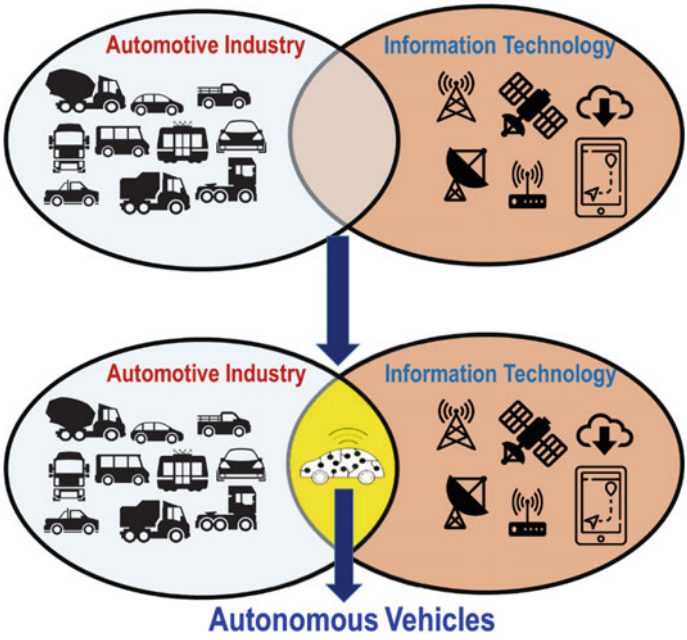

Fig. 1.1 The merging of the automotive and information industries

enormous number of electronic and communication devices that created connected the automotive safety with the need for security. As we can see in Fig. 1.1 has shown the automotive industry integrated with information technology and working to develop Intelligent vehicles. This merging has made the fantasy of an autonomous vehicle conceivable soon. Nevertheless, even in the present vehicles we get a wealth of real-time information in regard to fuel and ignition systems, power trains, brakes, transmissions, electronic and demonstrative hardware alongside parking, indicators, street risk alerts, voyage control, and route help.

Soon we are heading to complete automation that means an end-to-end automotive journey without driver intervention. In is scenario, the driver becomes the passenger! This idea was science fiction a few decades ago. The 1980s sci-fi show "Knight Rider" acquainted with the overall population the possibility of a self-sufficient vehicle named "KITT" or Knight Industries Two Thousand as shown in Fig. 1.2. The "KITT" had three modes: Normal Cruise, Auto Cruise and Pursuit [2].

- At Normal Cruise, the driver had control of the vehicle. In a crisis, the vehicle could dominate and enact Auto Cruise mode however there was a "Manual Override" to forestall this.
- At Auto Cruise, the vehicle could drive itself using a propelled Auto Collision Avoidance System.

Fig. 1.2 Knight Industries Two Thousand (KITT) autonomous car

- At Pursuit Mode, the vehicle was utilized during rapid driving circumstances and utilized a mix of manual and PC helped activity. The driver was in fact in charge of the vehicle and the PC helped direct certain moves.
- It is fascinating to take note of that in Normal Cruise, the driver had control of the vehicle yet in a crisis, the vehicle could even now dominate and actuate Auto Cruise mode indicating that innovation was better than the human information.

In any case, there was a "Manual Override" to forestall if the driver decides to do so uncovering an innate doubt to the new technology. In Fig. 1.3 has represents the connectivity of advanced vehicle of things (AVOT). It's means as much as vehicles

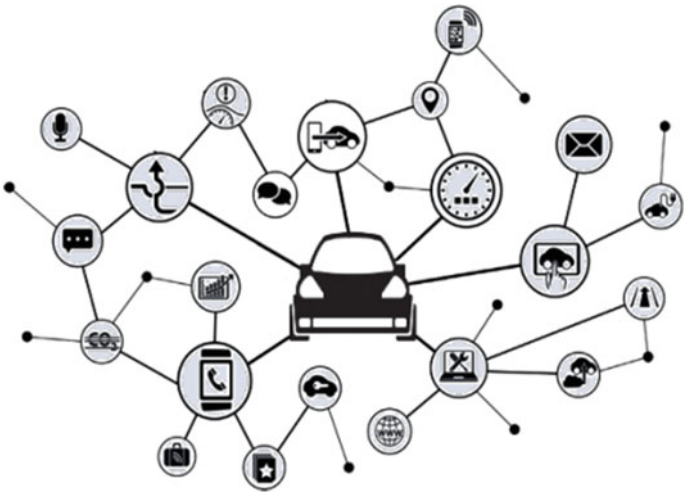

Fig. 1.3 Connectivity of advanced vehicles of things (AVOT)

are integrating with information technology as much as they are connected with things such as phone, watches navigations, service center as many as can.

The rest of the chapter is organized as follows. Section 1.2 provides an overview of automotive technology components. Section 1.3 introduces the International SAE level development of vehicle automation technology and related characteristics. Section 1.4 discusses the information security of automotive applications. Section 1.5 conclude an overview of current available automotive vehicle application and future research directions.

1.2 An Overview of Automotive Technology Components

A close examination of any current vehicle will reveal that in years that are more recent the automotive industry has been drastically augmented from mechanical and driver-only physical controls to Electronic Control Units or ECUs. There are dozens of embedded ECUs in modern vehicles that control electronic components running millions of lines of code. These units are well connected over internal buses (mainly CAN buses) to enable both critical safety and convenience features [3]. Some functionality examples include engine control, brakes, steering, phone connectivity, Bluetooth, connectivity for alerting the driver, oil pressure warnings, engine efficiency information, and voice control of car functions. Let us examine in even more detail what the merging of the automotive industry with the information technology industry has provided us so far. In Fig. 1.4 has explained the four major areas Electronics Control Units (ECUs) and other high-tech equipment controls in vehicles.

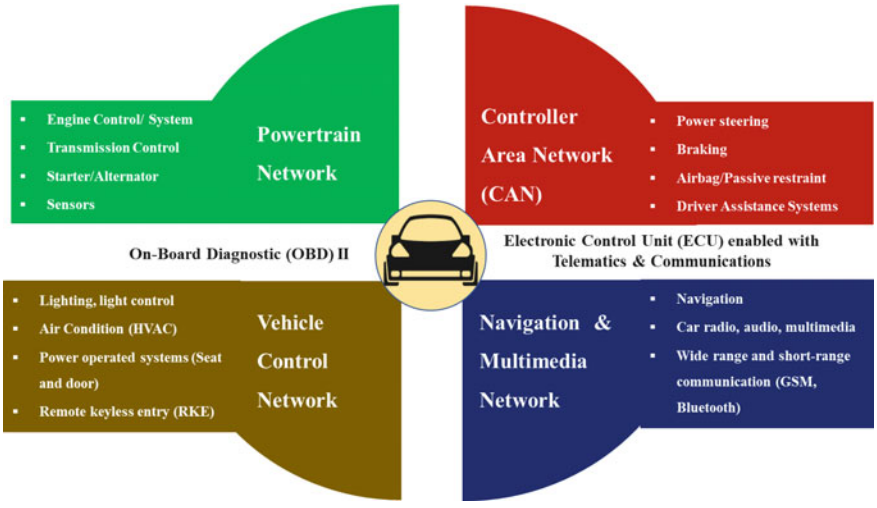

Fig. 1.4 Advanced automotive technology components

These are power train Network, the Controller Area Network (CAN), the vehicle network, and the navigator and multimedia network.

- ***The Powertrain Network*** permits connectivity between ECUs in the vehicle and guarantees that the engine control unit coordinates appropriately. The transmission control framework guarantees that engine torque yield is effectively moved to the street giving the traction and gives control the driver requires.
- ***The Controller Area Network (CAN)*** is a fast half-duplex differential and sequential communication protocol. It is utilized as multi-master system for interfacing ECUs inside the vehicle.
- ***The Navigation and Multimedia Network*** gives infotainment frameworks in the zones of wide range and short-range communication and navigation ***The Vehicle Control Network*** progresses technology and gives better coordination between vehicle and driver.
- ***The On-Board Diagnostic (OBD) II*** is the second generation of On-Board Self-Diagnostic. It is utilized for all sort of vehicles to give cooperation among equipment and programming in the vehicle's PC to monitor virtually every part. We will get more insights regarding OBD II later in this course. Finally, the ***Electronic Control Unit (ECU)*** empowered with Telematics and Communications gives the availability and information transmission between numerous buses.

1.3 Level of Vehicle Automation

SAE International, previously known as the Society of Automotive Engineers, is a U.S. based globally active professional association and standards developing organization. On your screen, you can see the updated chart they released in 2019, defining the six levels of driving automation from SAE level 0 (no automation) to SAE level 5 (full vehicle autonomy). This chart serves as the industry's most-cited reference for automated vehicle (AV) capabilities. It is predicted that by 2030 automotive technology will be fully autonomous. In Fig. 1.5 has shown the description of vehicle automation levels [4].

- ***Level 0—No Automation***
  At level 0 there is no automation, and the vehicle is controlled physically by the human driver including all parts of speed and direction. Some features, for example, the emergency braking mechanism is accessible in level 0 vehicle, yet it is not automated. Figure 1.6 has presents the level 0 vehicles.
- ***Level 1 Driver Assisted***: Level 1 the driver gets support for particular tasks, for example, parking, and indicators; level 1 has presented the automation feature cruise control. Another example, versatile cruise control, ensures there is a safe separation between vehicles however, the human driver monitors and controls the driving function, for example, speed, controlling, and slowing down. Figure 1.7 shown the vehicles of level 1.

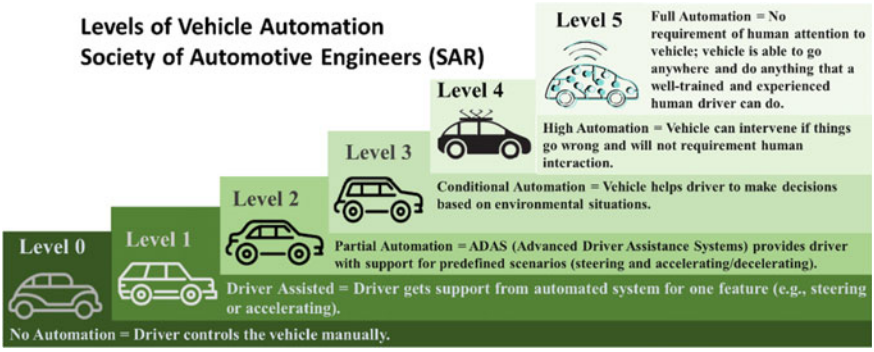

Fig. 1.5 Levels of vehicle automation

Fig. 1.6 Level 0 vehicle example

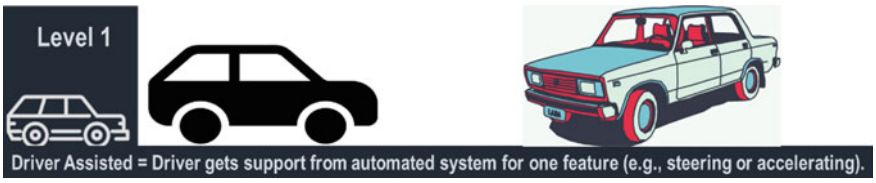

Fig. 1.7 Level 1 vehicle example

- ***Level 2—Partial Automation***: Level 2 vehicles have embraced the advanced driver assistance systems (ADAS) where the driver gets some help for adapting to predefined situations because of in-vehicle sensors and different electronics that illuminate the vehicle to separate with different vehicles. Speed, focusing the vehicle on the path, and so on. ADAS can control the steering and accelerate or decelerate on the continuous moving vehicles however the human driver can assume responsibility for the vehicle whenever. Some development has been made through the journey of automation and some of them in level 2 vehicles: Tesla Autopilot, Cadillac (General Motors) Super Cruise frameworks. An overview of ADAS based vehicle has shown in Fig. 1.8.

Fig. 1.8 Level 2 ADAS enabled vehicle example

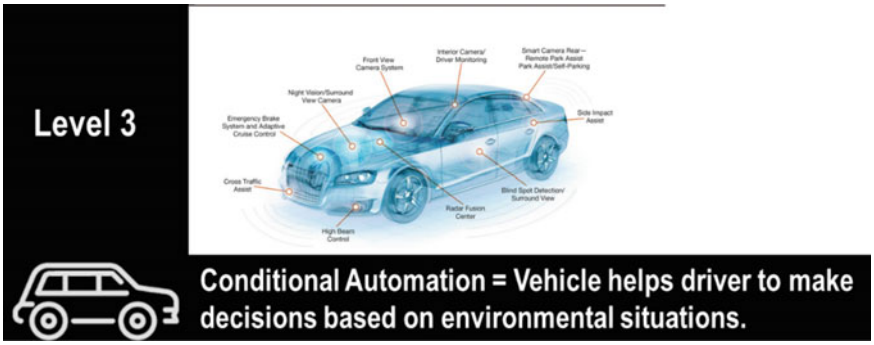

Fig. 1.9 Level 3 vehicle example

- ***Level 3—Conditional Automation***: Vehicles of this level have a superior comprehension about their environment since they identify things around and make better choices. A driver can give up control to an automated system however should be prepared to reclaim control; for instance, a level 3 vehicle will decelerate in high rush hour traffic and quicken in low rush traffic. Examples of a level 3 vehicle: Audi A8L in Europe (2019) as presented in Fig. 1.9.
- ***Level 4—High Automation***: Level 4 vehicles need not bother with any human mediation largely however human drivers have the alternative to drive physically. The principle key distinction between level 3 and level 4 is that level 4 vehicles can intervene on the off chance that anything unordinary ought to occur or turn out badly. Level 4 vehicles can run in self-driving mode yet because of unsupported infrastructure it works inside restricted or limited areas. Examples of level 4 vehicles: NAVYA (French organization) shuttles. Cabs in the U.S., and WAYMO self-driving taxi in Arizona (from Google) shows in Fig. 1.10.
- ***Level 5—Full Automation***: At Level 5 we show up a genuine driverless vehicle. Level 5 able vehicles utilize an automated driving system (ADS) in the vehicle to monitor and move through all street conditions and require no human intercessions at all eliminating the requirement for a controlling steering wheel and pedal as well as conditional braking movement. The human occupants are simply travelers [5]. Although a significant number of the mechanical, parts exist for an artificially intelligent vehicle today, because of guidelines and legal battle in court. Level 5

Fig. 1.10 Level 4 vehicle example

Fig. 1.11 Level 5 fully automated vehicle example

vehicles are likely still a few years away (expected around 2030) and it is depicted in Fig. 1.11.

On the path to realizing a level 5 fully autonomous vehicle, several automotive technologies under development are coming soon to a parking lot near you. In the context of cyber security, we must be aware of these technologies, as they will become part of the final solution.

1.4 Information Security for Automotive Applications

Now there is a big question that whether current IT security is feasible for the future and current Automotive Technology and applications. Indeed, future automotive technology and applications will have a vital need for IT protection. Below are some advantages of IT security with reference to the embedded automotive systems. Some applications domains are listed in Fig. 1.12, where IT Security can play an effective and efficient role for Automotive Technology.

- IT security will enhance the reliability of the control systems in the automotive and can increase the fault tolerance of the Telematics systems.
- IT security can play a very efficient role in dealing with the novel innovations and technologies introduced in the Automotive.

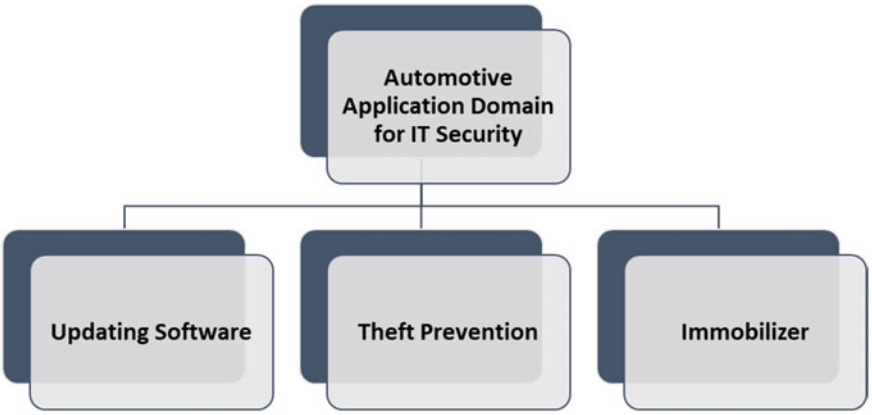

Fig. 1.12 Automotive application domain for IT security

- **Updating Software**: There is a need to update the Electronic Control Units (ECU) in the car because after the car is shipped many software errors are found in them. Secondly, many users want to configure their car according to their utility, comfort and price. There is some non-profiting updating for the manufacturers, where the owner updates a feature, which looks attractive, and with no cost payment. Embedded Security technologies such as Digital signature, encryption can restrict the user to feely update the software's according to his will.
- **Theft Prevention**: The electronic security device immobilizer was used way back to prevent is maybe the oldest type of IT security in Automotive and it has benefited by avoiding car thefts up to 60% over the last 15 years. Similar cryptography methods such as Identification protocols and tamper resistance protocols can be proposed for each part of the automotive to avoid them from being stolen or illegal exchange.
- **Immobilizer**: An immobilizer or immobilizer is an electronic security gadget fitted to an engine vehicle that halts the engine from running except if the right transponder key (or other tokens) is available. This keeps the vehicle from being "hotwired" after entry has been accomplished and hence reduces engine vehicle burglary. Examination shows that the uniform utilization of immobilizers diminished the pace of vehicle burglary by 40%.

Automotive systems are executed as a network of embedded smart devices, some of which have worldwide availability and established communication. Conventional vehicle security arrangements, similar to caution, keyless section, and so forth neglect to ensure the automotive IT security framework.

1.5 Automotive Vehicle Applications

New technologies need to connect with each other and bond seamlessly with the people utilizing them. Let us examine how this takes place in the next few paragraphs. A Connected car uses integrated information technology that is well equipped with a wireless network that communicates with other telecommunication systems. For example, a connected car will use the smartphone operating system and the telecommunications network operating standards to share information with other devices both inside and outside the vehicle. Next, there are groups of technologies that provide warnings to the driver. Advanced driver-assistance systems (ADAS) is one such example. ADAS will synchronize the data received from multiple resources, such as ECUs, cameras, and make driving decisions based on that data to accelerate, decelerate brake, etc.

Other technology is the Connected HD; these vehicles use data transmission within ECU CAN and sensors (such as protocol stacks, object detection, Ethernet and security image analysis, graphic processing, traffic signal recognition, etc.) to make decision so the vehicle drives smoothly on road. Autonomous vehicles have technology strategically positioned. This image identifies where each area of technology is positioned [6].

- **LIDAR and Radar Safety Sensors**

LIDAR estimates separation by enlightening targets with pulsed laser light and measure reflected pulses with sensors to make a 3-D guide of the region.

Cameras give real-time vehicle sideways collision i.e., obstacle recognition to encourage path takeoff and track street information (like street signs). Radar sensors monitor the situation of the vehicles close by. The Dedicated Short-Range Communications (DSRC) device license a vehicle to establish connections and communicate with different vehicles (V2V) utilizing a wireless communication standard that empowers reliable and trustworthy information transmission in active safety applications. The Central Computer gets data from different parts and coordinates vehicle largely. Ultrasonic Sensors utilize high-frequency sound waves generated from an attached sensor in the vehicle framework that bobs back to compute separation between vehicles on the road and obstacles. GPS draws the pattern of the vehicle utilizing satellites and wholly designed in triangular pattern. Either current GPS technology is constrained to a specific separation vehicles or obstacles, yet propelled GPS is being developed. Figure 1.13 has demonstrated the case of innovation situating in innovative vehicles design. The position can change the spot as per manufacturing organization.

- **Google Autonomous Vehicle**

In addition to the technology in an autonomous vehicle, each vehicle will have different sensors positioned to assist in maneuvering the vehicle. This image is a 3D rendering of an autonomous self-driving electric car using LIDAR and Radar Safety sensors. Notice the three Emergency Braking sensors in the front of the vehicle, the

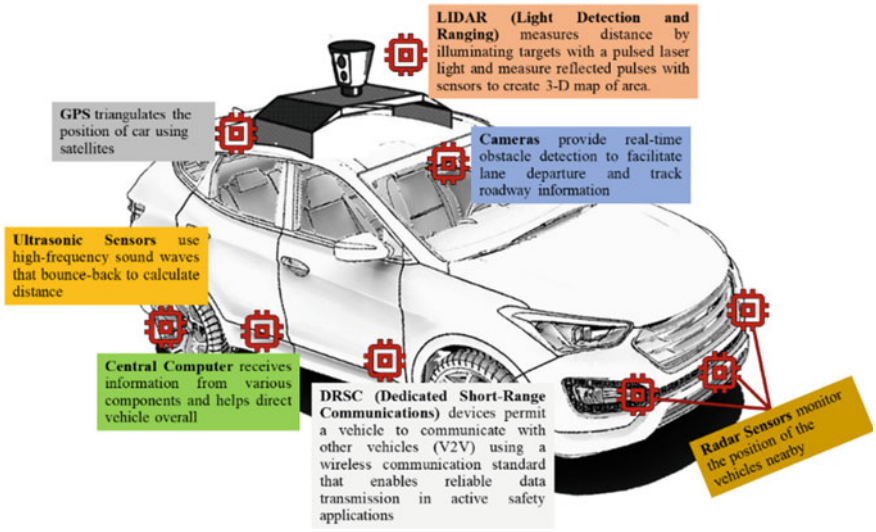

Fig. 1.13 An example of technology positioning in vehicles

three Parking Aid System sensors in the rear bumper of the vehicle, and the four Blind Spot Detection sensors on the sides of the vehicle that will assist in switching lanes [7].

In Fig. 1.14 has shown a working example of a Google's self-driving car. On the top of the vehicle, there are sensors such as lasers, radars and cameras that detect other cars and objects in all directions. The rounded shape of the vehicle is rounded not so much for aerodynamic reasons but to allow for maximum sensor field of view [8]. The interior is designed with the premise that everybody is a passenger meaning it is designed for riding not driving [9]. The on-board computer is quite unique in the sense that it has been designed and built for the sole purpose to accommodate self-driving. In the Google self-driving car, battery banks provide the power as the vehicle is 100% electric. Lastly, the back-up systems provide redundant systems for steering and braking.

A well-established standard is consistently an assurance that procedures and usage are agreeable with best practices and rules. A few endeavors have just been attempted to give such cyber security rules to the car business, universally yet additionally nation explicit. The covering hazard is a reality, and all these normalization bodies need to arrange with one another to maintain a strategic distance from clashes and ambiguities. Nearby activities incorporate for example the EVITA (E-Safety Vehicle Intrusion Protected Applications) venture in Europe, which planned to give in-vehicle reference engineering dependent on HSM. The Japanese IPA (Information Promotion Agency) vehicle data security direct secured a start to finish lie-pattern of the vehicle including outsider and providers conduct toward security. Even more as of late, universal normalization bodies, for example, ISO (International Organization for Standardization) and SAE (Society of Automotive Engineers) joint their push to

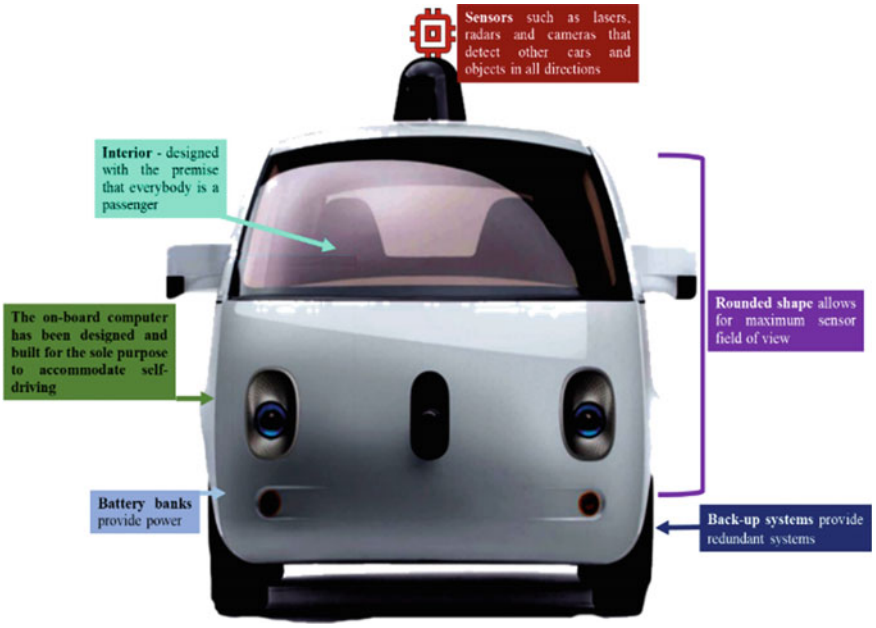

Fig. 1.14 Example: Google autonomous vehicle [8]

deal with the meaning of a devoted cyber security standard for the car business. SAE as of now started these works inside the Vehicle Electrical System Security Committee where the J3061 cyber security manual and the J3101 prerequisites for equipment ensured security archives are delivered. ISO's TC22 and SAE are likewise recognizing the possible communications between framework wellbeing and cyber security.

1.6 Conclusion

In this chapter, presents the history of automotive technology that is included in six layers. Which begins with layer 0 it has manual vehicle to Layer 5 that is full automation. The advanced components of vehicles is On-Board. Electronic Control Unit etc. has described with example of Self-driving car. With the huge changes that will go with the presentation of ADS in an expanding scale, it very well may be foreseen that recognizable impacts will occur on user experience, traffic wellbeing, effectiveness, portability, efficiency, energy, environment, and economy. It is additionally obvious that ADS will cause unpleasant problematic changes in certain businesses, and the arrangement way may not be as convenient and smooth as certain defenders may want. Building up an all-around grounded and methodical assessment system and

making reasonable and down to earth devices to examine the social advantages of ADS stay a difficult yet commendable theme for future projects.

Acknowledgements This research was funded by Woosong University Academic Research in 2021.

References

1. G. Ur-Rehman, A. Ghani, M. Zubair, S.H.A. Naqvi, S. Muhammad, D. Singh, IPS: incentive and punishment scheme for omitting selfishness on the internet of vehicles (loV). IEEE Access (2019). https://doi.org/10.1109/ACCESS20192933873
2. Knight Rider (2008 film), https://en.wikipedia.org/wiki?curid147467112008
3. The 5 Levels of Autonomous Vehicles (2018), https://www.truecar.com/blog/5-levels-autonomous-vehicles/
4. SAE J3016, Levels of Driving Automation (2019), https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic
5. Sunil Raj Thota Blog, Wanna go for a long ride cars. Let's Kickstart the 'Driving Innovation—Self-driving'. https://sunitrajthota.blogspot.com/201904wanna-go-for-long-ride-lets-kickstart-the-driving-innovation-self-driving-carshtml (2019)
6. R.P. Prakash, R. Tripathi, D. Singh, Analytical model for clustered vehicular ad hoc network analysis. ICT Express (2018). https://doi.org/10.1016/j.icte.2018.01.001
7. D. Singh, G. Tripathi, S.C. Shah, R. da Rosa Righi, Cyber-physical surveillance system for the internet of vehicles, in *JEEE World Forum on Internet of Things WF-IoT 2018*, Singapore, 5–8 Feb 2018, pp. 551–555
8. M. Singh, IEEE E-Learning, Evolution of intelligent and autonomous vehicles (2020). https://ieeexplore.ieee.org/courses/details/EDP585
9. D. Singh, M. Singh, Internet of vehicles for smart and safe driving, in *2015 International Conference on Connected Vehicles and Expo (ICCVE)*, Shenzhen, China, 19–23 Oct 2015, pp. 328–329 (2015)