- Technologies for data anonymity addressing privacy concerns
- Dealing with critical latencies, e.g. in control loops
- System partitioning (local/cloud based intelligence)
- Mass data processing, filtering and mining; avoid flooding of communication network
- Real-time Models and design methods describing reliable interworking of heterogeneous systems (e.g. technical / economical / social / environmental systems). Identifying and monitoring critical system elements. Detecting critical overall system states in due time
- System concepts which support self-healing and containment of damage; strategies for failure contingency management
- Scalability of security functions
- Power grids have to be able to react correctly and quickly to fluctuations in the supply of electricity from renewable energy sources such as wind and solar facilities.

3.3.3 Smart Mobility and Transport

The connection of vehicles to the Internet gives rise to a wealth of new possibilities and applications which bring new functionalities to the individuals and/or the making of transport easier and safer. In this context the concept of Internet of Vehicles (IoV) [102] connected with the concept of Internet of Energy (IoE) represent future trends for smart transportation and mobility applications.

At the same time creating new mobile ecosystems based on trust, security and convenience to mobile/contactless services and transportation applications will ensure security, mobility and convenience to consumer-centric transactions and services.

Representing human behaviour in the design, development, and operation of cyber physical systems in autonomous vehicles is a challenge. Incorporating human-in-the-loop considerations is critical to safety, dependability, and predictability. There is currently limited understanding of how driver behaviour will be affected by adaptive traffic control cyber physical systems. In addition, it is difficult to account for the stochastic effects of the human driver in a mixed traffic environment (i.e., human and autonomous vehicle drivers) such as that found in traffic control cyber physical systems. Increasing integration calls for security measures that are not physical, but more logical while still ensuring there will be no security compromise. As cyber physical systems become more complex and interactions between components increases, safety and security

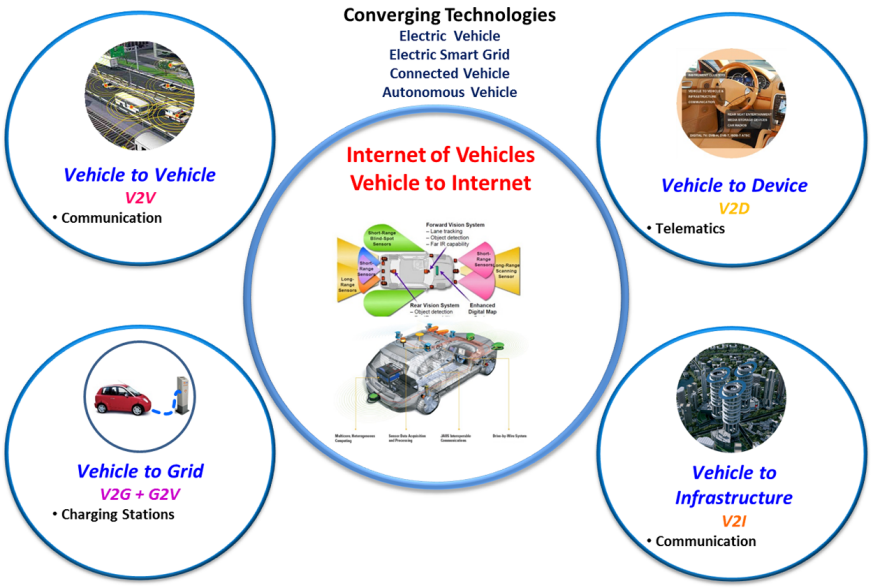

Figure 3.24 Technologies Convergence – Internet of Vehicles Case

will continue to be of paramount importance [83]. All these elements are of the paramount importance for the IoT ecosystems developed based on these enabling technologies.

When talking about IoT in the context of automotive and telematics, we may refer to the following application scenarios:

- Standards must be defined regarding the charging voltage of the power electronics, and a decision needs to be made as to whether the recharging processes should be controlled by a system within the vehicle or one installed at the charging station.
- Components for bidirectional operations and flexible billing for electricity need to be developed if electric vehicles are to be used as electricity storage media.
- **IoT as an inherent part of the vehicle control and management system**: Already today certain technical functions of the vehicles' on-board systems can be monitored on line by the service centre or garage to allow for preventative maintenance, remote diagnostics, instantaneous support and timely availability of spare parts. For this purpose data from on-board sensors are collected by a smart on-board unit and communicated via the Internet to the service centre.

- **IoT enabling traffic management and control**: Cars should be able to organise themselves in order to avoid traffic jams and to optimise drive energy usage. This may be done in coordination and cooperation with the infrastructure of a smart city's traffic control and management system. Additionally dynamic road pricing and parking tax can be important elements of such a system. Further mutual communications between the vehicles and with the infrastructure enable new methods for considerably increasing traffic safety, thus contributing to the reduction in the number of traffic accidents.
- **IoT enabling new transport scenarios (multi-modal transport):** In such scenarios, e.g. automotive OEMs see themselves as mobility providers rather than manufacturers of vehicles. The user will be offered an optimal solution for transportation from A to B, based on all available and suitable transport means. Thus, based on the momentary traffic situation an ideal solution may be a mix of individual vehicles, vehicle sharing, railway, and commuter systems. In order to allow for seamless usage and on-time availability of these elements (including parking space), availability needs to be verified and guaranteed by online reservation and online booking, ideally in interplay with the above mentioned smart city traffic management systems.
- **Autonomous driving and interfacing with the infrastructure (V2V, V2I):** The challenges address the interaction between the vehicle and the environment (sensors, actuators, communication, processing, information exchange, etc.) by considering road navigation systems that combines road localization and road shape estimation to drive on roads where a priori road geometry both is and is not available. Address a mixed-mode planning system that is able to both efficiently navigate on roads and safely manoeuvre through open areas and parking lots and develop a behavioural engine that is capable of both following the rules of the road and avoid them when necessary.

Self-driving vehicles today are in the prototype phase and the idea is becoming just another technology on the computing industry's parts list. By using automotive vision chips that can be used to help vehicles understand the environment around them by detecting pedestrians, traffic lights, collisions, drowsy drivers, and road lane markings. Those tasks initially are more the sort of thing that would help a driver in unusual circumstances rather than take over full time. But they're a significant step in the gradual shift toward

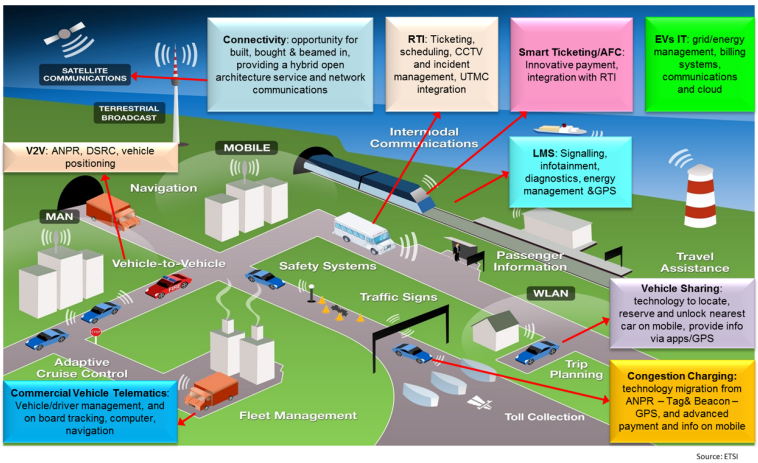

Figure 3.25 ITS Ecosystem (Source: ETSI)

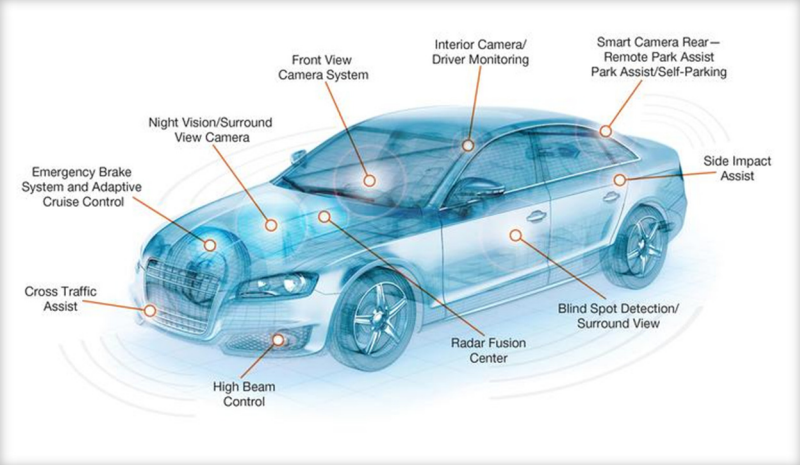

Figure 3.26 Communication and computer vision technologies for driver-assistance and V2V/V2I interaction [80].

the computer-controlled vehicles that Google, Volvo, and other companies are working on [80].

These scenarios are, not independent from each other and show their full potential when combined and used for different applications.

Technical elements of such systems are smart phones and smart vehicle on-board units which acquire information from the user (e.g. position, destination

Figure 3.27 Internet of Vehicles Concept

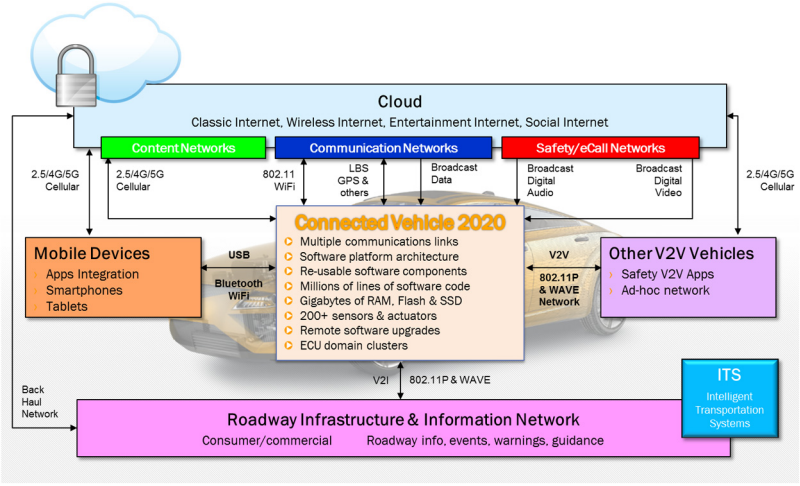

Figure 3.28 Connected Vehicle 2020-Mobility Ecosystem (Source: Continental Corporation)

and schedule) and from on board systems (e.g. vehicle status, position, energy usage profile, driving profile). They interact with external systems (e.g. traffic control systems, parking management, vehicle sharing managements, electric vehicle charging infrastructure). Moreover they need to initiate and perform the related payment procedures.

The concept of Internet of Vehicles (IoV) is the next step for future smart transportation and mobility applications and requires creating new mobile ecosystems based on trust, security and convenience to mobile/contactless services and transportation applications in order to ensure security, mobility and convenience to consumer-centric transactions and services.

Smart sensors in the road and traffic control infrastructures need to collect information about road and traffic status, weather conditions, etc. This requires robust sensors (and actuators) which are able to reliably deliver information to the systems mentioned above. Such reliable communication needs to be based on M2M communication protocols which consider the timing, safety, and security constraints. The expected high amount of data will require sophisticated data mining strategies. Overall optimisation of traffic flow and energy usage may be achieved by collective organisation among the individual vehicles. First steps could be the gradual extension of DATEX-II by IoT related technologies and information. The (international) standardisation of protocol stacks and interfaces is of utmost importance to enable economic competition and guarantee smooth interaction of different vendor products.

When dealing with information related to individuals' positions, destinations, schedules, and user habits, privacy concerns gain highest priority. They even might become road blockers for such technologies. Consequently not only secure communication paths but also procedures which guarantee anonymity and de-personalization of sensible data are of interest.

Some research challenges:

- Safe and secure communication with elements at the network edge, inter-vehicle communication, and vehicle to infrastructure communication
- Energy saving robust and reliable smart sensors and actuators in vehicles and infrastructure
- Technologies for data anonymity addressing privacy concerns
- System partitioning (local/cloud based intelligence)
- Identifying and monitoring critical system elements. Detecting critical overall system states in due time
- Technologies supporting self-organisation and dynamic formation of structures / re-structuring
- Ensure an adequate level of trust and secure exchange of data among different vertical ICT infrastructures (e.g., intermodal scenario).