CAR-Evolution

Mobility, Connectivity & Big Data meet Cyber

Ralph D. Thiele

March 2016

Abstract

Cars of the future will be very different from the ones we have known. New technologies along with the growing interest of customers in new services have started altering business models that have excelled for more than a century. The car of the future will be connected. Vehicles will communicate with each other and with the infrastructure. The connected car will play a major role in a dynamically growing ecosystem of connected devices and systems.

With view to seamless connectivity automakers will need to fundamentally rethink the role of IT and further technology capabilities they will need in the future. Information and Communication Technology has become a critical enabler. Connectivity and Big Data have come to the fore. Cyber security becomes a prominent issue as connected cars can be hacked.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is objective and task oriented, and impartial to party politics.

In an ever more complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, that bring major opportunities but also risks, decision makers in enterprises and politics depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics relating to politics, economy, international relations, and security/defence. ISPSW network experts have operated in executive positions, in some cases for decades, and command wide-ranging experience in their respective areas of specialization.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analysis

1. Urban Mobility

The car of the future will be connected. The systematic introduction of "cooperative systems" in which vehicles communicate with each other and with the infrastructure and where driving can even be automated promises significant improvements in road safety. In particular, the complex traffic systems of cities will profit. Features such as real-time traffic reports, upcoming roadside attractions, and remote vehicle location services are just some of the many opportunities available to personalize a drivers' experience.

The connected car will play a major role in a dynamically growing ecosystem of connected devices and systems. With the world's population growing and becoming more urbanized, urban mobility requirements will drive future developments. This will be a tough challenge for cities around the globe as existing mobility systems are already inadequate, while urbanisation and increasing populations continue to increase demand. Cities have traditionally sought to solve such challenges by adding new capacity to match demand. Obviously, this approach is neither efficient nor sustainable.

On top of the growing demand, mobility needs are changing and evolving, and travellers' expectations of seamless movement are becoming ever greater. In our connected society, people expect features that buyers expect, such as Bluetooth, Internet access, GPS and lifestyle guides or virtual personal assistants in their modern vehicles. Many new mobility solutions are emerging, which leverage technology to improve service provision and manage demand. Consequently, a holistic response to urban mobility needs to seek proper balances between supply and demand in order to facilitate more sustainable outcomes. To this end Smart City concepts are aiming at efficient solutions.

Information and Communication Technology has become a critical enabler in Smart City concepts to move the masses more efficiently and safely. Among the key emerging trends within Smart Cities is the move towards a holistic approach, where city systems such as transport, energy, water, waste, housing and planning are brought together in an integrated fashion. Plenty of information is already available in the cloud – a perfect precondition to avoid getting stuck in construction zones, traffic jams, and accident scenes. When combined with infrastructure data from parking garages, toll gates, traffic signals, this will provide a broader perspective. The auto industry is projecting a good business opportunity related to interactive urban transport systems in the expectation that Smart Cities projects are likely to promote business opportunities in the connected car segment.

Data will play an increasing important role in this development. Through the use of real-time systems and sensors, data are collected, evaluated and then processed in real-time or at least near real-time in support oft he driver. Connected cars will communicate with each other, with their drivers, their manufacturers, their surroundings, and with a variety of service providers. Development, production, sales and customer service in the automotive sector – all will be effected.

Apparently, the connected car technology will guide mobility step by step into automated driving.[1] As cars start talking to each other such vehicles will eventually be driving themselves. Although automakers and tech com-

[1] BMW is preparing its 5 Series self-driving prototype. Google is testing its self-driving cars on roads. Daimler is testing an automated series-production truck on the highway in Germany. Qualcomm and Mercedes-Benz have partnered concerning the 2016 Mercedes F 015 self-driving car. Google and Ford have focused on electric vehicle (EV) and autonomous vehicle (AV) technology. The two companies have teamed up and plan to form a new enterprise.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

panies have shown measured progress here, there is still a long way to go. Aside from technological hurdles currently, there are plenty of legislative details to sort through.

2. Connectivity and Big Data

Connected car applications such as telematics, driver assistance, and infotainment require seamless connectivity. Connectivity will enable a broad collection of new features, thus transforming not only how we drive, but also how we buy and maintain cars, and how automakers sell them. Connected cars are built with embedded computers called electronic control units. These are connected to sensors for data acquisition and further in-vehicle network. The vehicles exchange data with external sources via Bluetooth, Wi-Fi, 3G, and LTE networks. The advent of vehicle-to-vehicle and vehicle-to-infrastructure communication as the connected car communicates and collaborates with other cars, but also with traffic lights, parking bays and retailers has increased this trend. The respective integration of information and consumer electronics into the car and ensuring connectivity among them is one of the biggest challenges.

The connected car will generate masses of data. It captures data on the operation of individual components of the vehicle running this data through sophisticated algorithms permits preventive diagnostics. But by leveraging the wealth of data generated by vehicle sensors, vehicle applications and driver interactions, it also becomes possible to generate insight-driven improvements to marketing, sales, service and product development functions, to personalize and deepen customer relationships, and to increase revenue by developing differentiated value-add services. Thus the effective management of data services will become the core to deploying smarter transportation solutions and new revenue-generating services.

Big Data offers new opportunities and fields of enterprise. With the rapid growth in data, the tools for processing and analysing mass data have developed. Big Data refers specifically to large amounts and various types of data, especially unstructured data as well, which cannot be processed and analysed adequately using established databases and analysis tools.

As Big Data also comprises mobility- and location-based services, it becomes possible to offer mobile support for trip planning and the management of real-time traffic and weather data. This, in combination with personal calendar data, enables a whole new service gradually turning automakers into mobility providers. Soon dealers will be able to control and optimize utilization levels at their repair shops by offering customers a discount for making an appointment at a time that suits the dealership. New services such as the tracking and immobilizing of stolen vehicles enable insurance companies to offer drivers of connected cars tailored, less expensive rates. Proactive customer management will aim to retain the loyalty of customers. Thus automakers will likely develop vehicle-specific services.

Industry is facing considerable change. Already today, the automotive establishment has taken a deep dive into the digital world. Carmaker giants like GM, Ford, Mercedes and BMW have been investing significantly in connected car technology. Automakers and tech giants have already begun to develop and introduce respective concepts. They have started reconsidering the car as a networked system. Services such as navigation, usage-based insurance, the stolen vehicle recovery (SVR), infotainment, remote diagnostic and self-diagnostic will soon drive the market.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Major automakers have apparently realized that there is relevant knowledge outside their own industry, particularly in the Information and Communication Technology industry and have started new partnerships.[2] Apple and transportation tech rivals such as Google, Tesla and Uber drive the vision of self-controlled, clean energy-powered pod cars that pick drivers up on demand. Traditional car manufacturers have started rushing to keep pace. Envisaged breakthroughs in electric vehicles, autonomous vehicles and shared transportation services – while urban populations are booming – may likely represent a turning point for the predominant model of personal car ownership, and the environmental impacts that come with it.

Already today many automotive, high tech, and telecom business leaders are competing in the connected car market by providing and developing innovative products and services. Toyota has created a new department to unify its connected car technologies. Verizon has launched its Internet of Things platform ThingSpace to simplify the development and deployment of the connected car applications. Samsung has partnered with leaders across industries to promote its connected car solution.

Patent information provides further valuable insights in upcoming developments. More than 1,000 published patent applications and issued patents in the USPTO as of January 31, 2016 are related to connected car and vehicular communication system and reflect the striking dynamics of innovation. More than 450 patents of these applications are selected as the key patents for the connected car applications and vehicular communication system. A significant number of these patent applications is owned by market leaders such as Cisco, Continental, and GM. The connected car accident avoidance system is also object of a large number of patent applications owned by several key market leaders such as Nissan, Toyota, and Honda and American Vehicular Sciences, an active patent monetizing entity.

3. Security by design

Connectivity can be hacked. In fact, car-hacking may become a major risk for connected cars. Design failure, criminal and other activities may threaten vehicle operation and put drivers and passenger's safety at risk. Consequently, the connected car must be protected, patched and updated in order to eliminate vulnerabilities and respond to threats as it becomes possible for an attacker to alter vehicle software for example by uploading malicious settings. The network connection can expose critical operational and safety systems, such as vehicle health diagnostics and automatic braking. There is a risk for access to vehicle data via connectors and in-vehicle app platforms, which will provide access for 3rd party developers to run applications inside the vehicle. The same applies to current smartphone integration technologies.

The shift to the connected car will require that automakers rethink the role of their IT department and the technology capabilities they will need in the future. Until now, IT has served a primarily internal function, developing the extensive software every car needs to run. But connectivity will give IT a fully operational role, building and running the software that will enable the necessary connectivity and functionality for connected cars thus developing full impact on the value chain of OEMs.

Particularly IT security has become a crucial precondition for the automotive industry in terms of a wider adoption of connected cars. One consequence will be to fully integrate back-office technology of IT departments with the technology they develop for the cars with view to IT security, the stability of technical systems and the

[2] An example is AT&T which has partnered with 10 automakers, including Porsche, Audi, Tesla, Jaguar Land Rover, and Volvo. It has also partnered with several automakers to add next-generation technology to their connected services. Additionally, AT&T and Porsche have entered a multi-year connected car agreement.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

design of the interaction between human beings and machines. With dozens of electronic control units and several in-vehicle bus systems as well as various wireless connections to the external world of a connected vehicle, it is vital to protect those systems in the best possible way against remote hacks, fraudulent attacks and any attempts that could affect traffic safety. This should include

- Aspects of data privacy and secure payments, secure infrastructures and communication channels are needed.
- Security infrastructures within the vehicle and from the vehicle to the backend infrastructures.
- Security intelligence within the vehicle, closely linked to security intelligence capabilities on the backend side, in order to detect attacks early and to avoid damages to the system.

A couple of further points come to mind:

- Seamless connectivity needs to be provided safe and secure over the entire vehicle's mobility envelope.
- Data encryption and the security of the telematics backend need to be primary concerns.
- Real-time detection becomes indispensable, alerts and prevention that are based on the analysis of both in-vehicle and out-of-vehicle communication.
- Software architecture should be designed with a plug-and-play approach to ensure support to new connectivity changes without altering the core software.

Cyber risks also include hardware. There is a serious danger that the supply chain for electronic components, including microchips, could be infiltrated. It is possible to alter the circuitry of the electronic components or substitute counterfeit components with altered circuitry that would contain malicious firmware and that would function in much the same way as malicious software.

As in cyber security the defender of an information space has a significant disadvantage, it is not sufficient to perform risk management for the own virtual information space only preventively and statically Risk management rather must be able to be adapted dynamically to the situation development. The focus needs to be on the availability of the information space and on the safeguarding of the integrity, reliability and confidentiality of the data and information.

Consequently, cyber risk management should provide for

- Precautions against immanent cyber threats to the own information space through prevention.
- Mitigating the effect of an attack through consequence management.

The primary prerequisite for an effective, proactive cyber risk management is a profound risk analysis with focus on the value chain and liabilities of an OEM and subsequently the build up of a comprehensive cyber situation picture, which should support a systematically proactive risk management.[3]

4. Conclusion

Cars of the future will be very different from the ones we have known. New technologies along with the growing interest of customers in new services have started altering business models that have excelled for more than a century. Already today, new driver assistance and safety systems can park the car autonomously, main-

[3] Radabaugh Gregory. "The Evolving Cyberspace Threat". JAPCC Journal Ed.15, p.65.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

tain a safe distance between cars at highway speeds, and warn drivers of hazards ahead. Communications and entertainment has made driving more comfortable and enjoyable than ever. Much more is to come.

Connected cars are on a fast lane. Their market has the potential to significantly boost revenues for automakers in the next years. Yet, success won't come by itself. All involved, to include law makers, car manufacturers, dealers, repair personnel and end users must adapt to new technological concepts and production methods not just to ensure the safety, efficiency and comfort of automobile drivers and passengers, but also to ensure their privacy and data security by design.

The shift to the connected car will require that automakers to fundamentally rethink the role of IT and further technology capabilities they will need in the future. They also must learn to bundle and sell the right mix of application and product packages in support of their customers. And they must systematically invest in research and development, particularly with view to connectivity, big data and cyber security to maintain technological leadership or may loose market shares soon.

***

Remarks: Opinions expressed in this contribution are those of the author. These remarks were given at the IQPC 2016 Automotive Cyber Security Conference in Berlin, Germany on March 21-24, 2016.

About the Author of this Issue

Ralph D. Thiele is Chairman of the Political-Military Society (pmg), Berlin, Germany and CEO at StratByrd Consulting. In 40 years of politico-military service, Colonel (ret.) Thiele has gained broad political, technological, academic and military expertise. He has been directly involved in numerous national and NATO strategic issues while serving as executive officer to the Bundeswehr Vice Chief of Defence Staff, Military Assistant to the Supreme Allied Commander Europe, in the Planning and Policy Staff of the German Minister of Defence, as Chief of Staff of the NATO Defense College, as Commander of the Bundeswehr Transformation Centre and as Director of Faculty at the German General Staff and Command College in Hamburg.

He has published numerous books and articles and is lecturing widely in Europe, Asia (Beijing, Seoul, Tokyo, and Ulaanbaatar) in the U.S. and Brazil on current comprehensive security affairs, cyber security, border security, maritime domain security, protection of critical infrastructure and defence and also historical issues.

Ralph D. Thiele is a member of the German Atlantic Association and member of the Defence Science Board to the Austrian Minister of Defence.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de