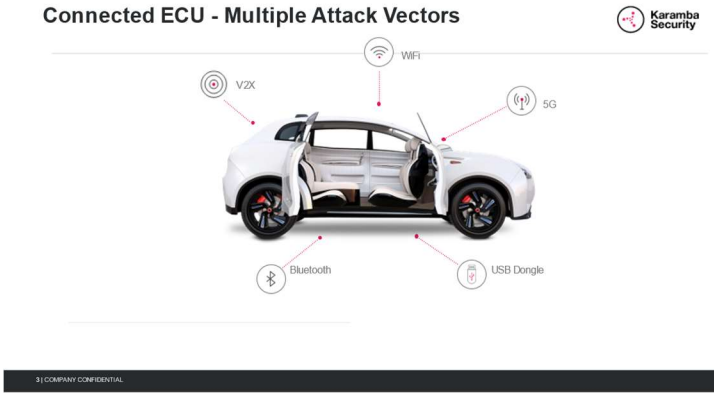
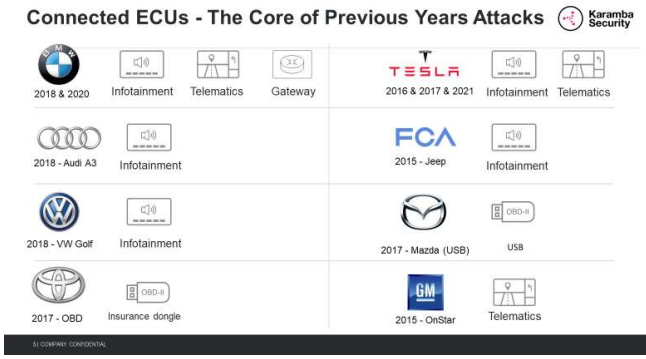
Licensing Executive Society International
Automotive Industry Advisory Board
Automotive Cybersecurity
Summary of Session Held September 22, 2021

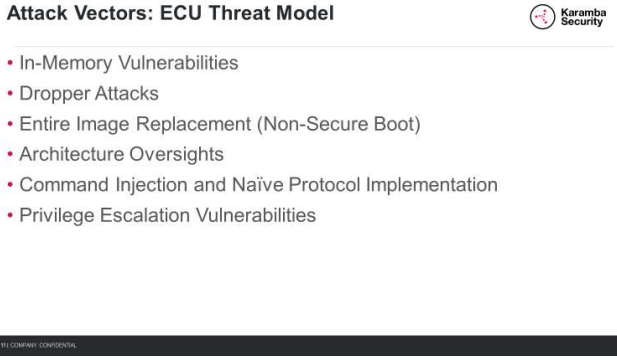
Background:

The connected car promises improved safety and convenience as the vehicle becomes an extension of our digital universe. As vehicles also become increasingly autonomous, data sharing with other vehicles in the "connected fleet" can help detect and avoid road hazards and traffic-induced delays. The connected vehicle universe (V2X) will deliver this new digital world to your car at 5G speeds in the not-so-distant future. These amazing connections hold significant promise for improved safety and convenience, but put vehicle systems at risk from outsiders with malicious intent. Hackers have multiple access points to deluge the vehicle with false commands, which presents risk to vehicle owners and manufacturers. Each electronic control unit (ECU) in the vehicle represents a potential target for hackers through messages delivered in a variety of ways:



Each point of access to the vehicle creates a vulnerability that must be managed against intrusion. The risk is real as evidenced by some very notable demonstrations:



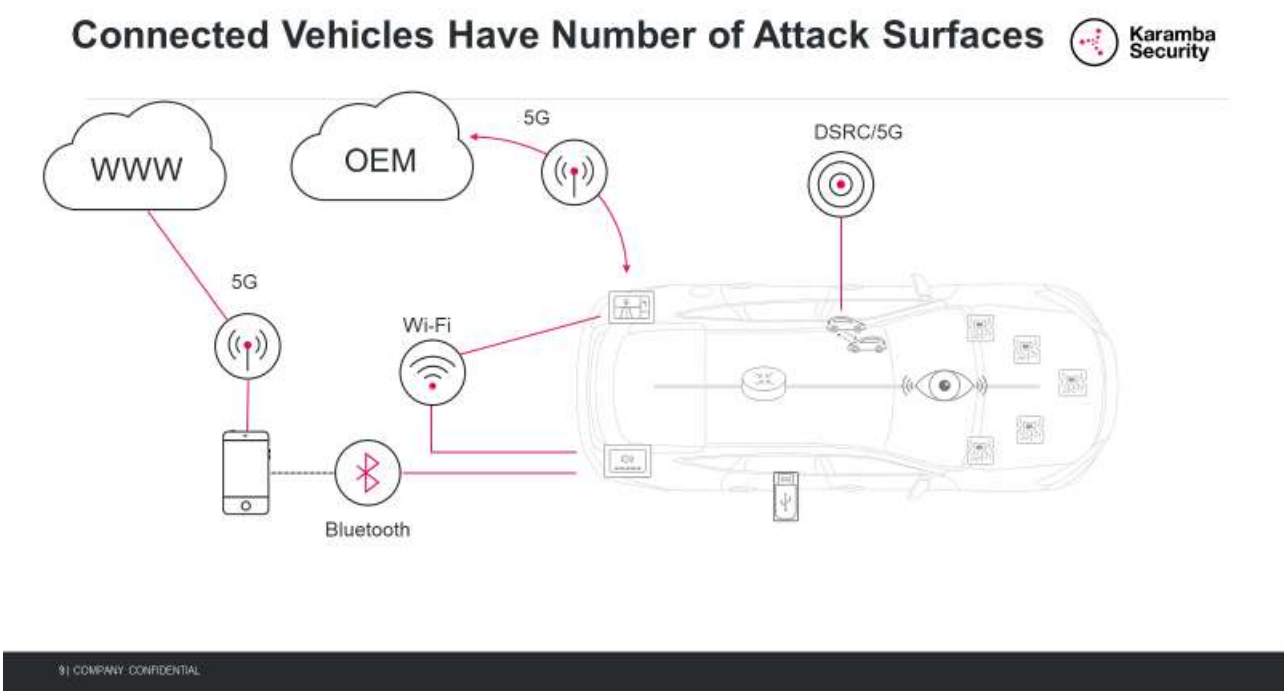


Intruders can target ECUs managing various critical safety and operational systems. As the number of electronically controlled systems grows, and with it the number of ECUs, vehicle connectivity creates a path for hackers to interfere with these critical systems. Electronic systems today control engine acceleration, vehicle braking, steering, air bag deployment, lighting, chassis controls, and a multitude of other key functions. As additional systems are added, increasing "self-guided/autonomous" operation of key systems and the vehicle, additional control functions will proliferate, increasing potential vulnerability.

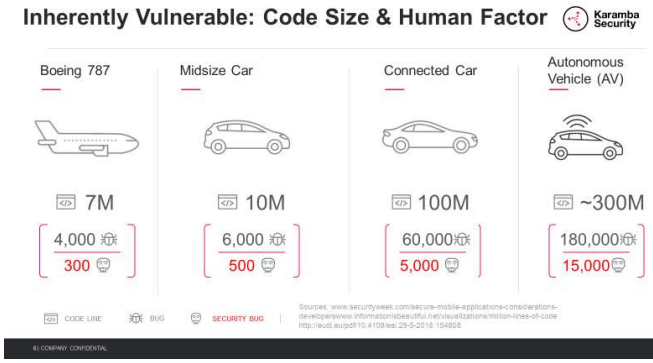
Vehicles first became connected to the outside world as a part of Formula 1 Racing. In the early 1980s, BMW aided Formula 1 race teams with real-time transmission of engine performance and vehicle dynamics data from vehicles on the

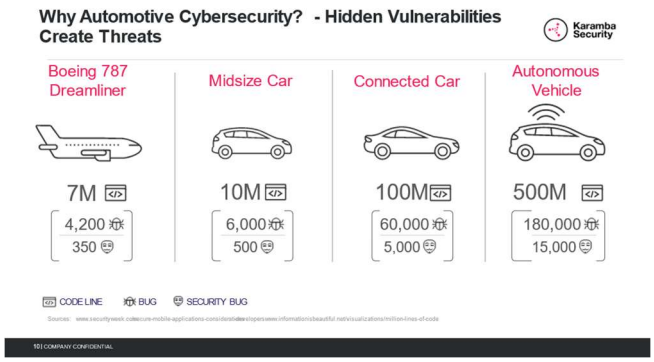
track. Wider application of technologies connecting consumer vehicles began with GM OnStar, introduced at the 1996 Chicago Auto Show. Emergency call systems were also introduced in 1996 to consumer vehicles in Europe. Early GM systems relied on CDMA (essentially 3G) communications backbone channels. GPS position detection for vehicles followed in the early 2000s when US President Bill Clinton allowed civilian applications to use the GPS satellite network. Around 2001 new vehicle connections allowed for remote vehicle diagnosis by vehicle OEMs. In 2004, BMW introduced systems with SIM cards, allowing drivers to access information from sources outside the vehicle for things like weather forecasts, messages, and traffic information. In 2008, Chrysler offered vehicle WiFi Hot Spots through an IPhone-based connection. Increased connectivity creates increasing numbers of paths for bad actors to penetrate the vehicle and generate messages that act on electronic control systems.

The following diagram summarizes how connected vehicle systems create vulnerabilities.



Software – Stored in vehicle ECUs or the cloud is the key to enabling system security and the source of potential issues. As vehicles become both connected and self- guided, millions of lines of computer code are added to vehicle control systems. This demand for new code creates the opportunity for bugs that can be exploited by potential hackers, as illustrated here:





With every major step toward full vehicle autonomy, the auto industry will deploy tens of millions of new lines of software into vehicle control systems. The task of writing this much new code is daunting, and many in the industry believe that open-sourced software provides part of the solution. This use of proven open-sourced code for key systems controls

offers both a solution and a challenge to vehicle developers. The ability to rapidly incorporate proven open-source code modules holds the promise of increasing speed of vehicle development. Re-use of open-source code components, however, also has the potential to proliferate code vulnerabilities repeatedly to a multitude of vehicle brands around the world. Said another way, if the same open-source code building blocks are used in multiple locations, and hackers learn how to exploit vulnerabilities in that code, the ability to hack multiple vehicle platforms simultaneously increases.

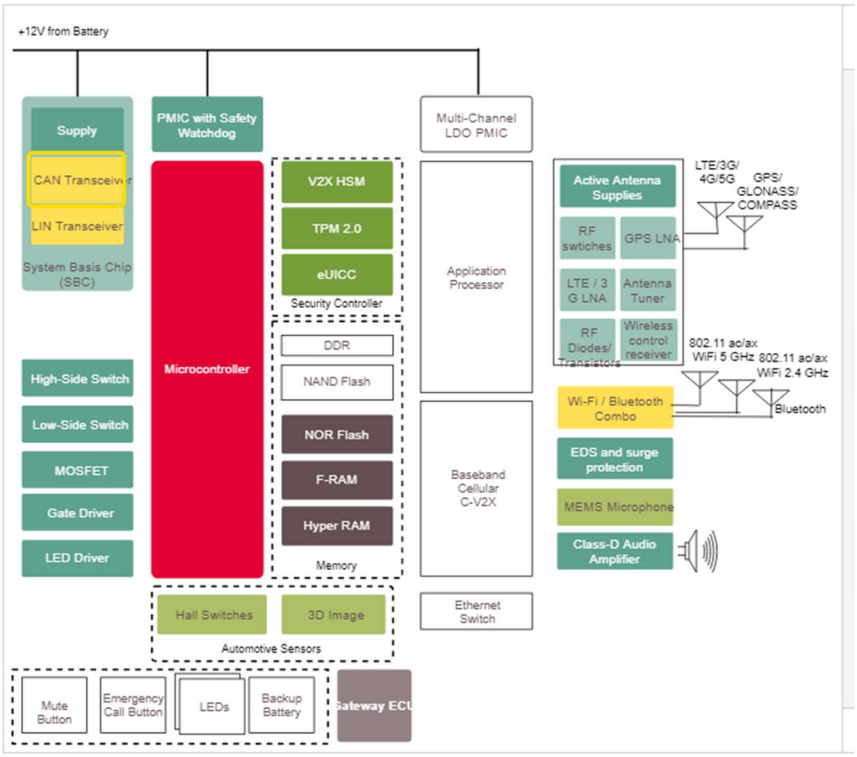
Hardware Technology

Protection from intruders most often comes in the form of software products used to safeguard access to key vehicle systems and authenticate messages received and acted on by vehicle control systems. These software products are resident in vehicle systems, in the cloud, and in OEM and fleet supervisory servers and central computing locations. Within the vehicle, software is present in key communications gateways, shown in this example.

Telematic Control Unit (TCU) - Acting as a Secure Gateway

Security for vehicle systems begins at the gateway where incoming messages are received. The following outlines the Telematic Control Unit (TCU), as shown on the Infineon website.

System diagram: Telematics control unit



https://www.infineon.com/cms/en/applications/automotive/automotive-security/telematics-control-unit/

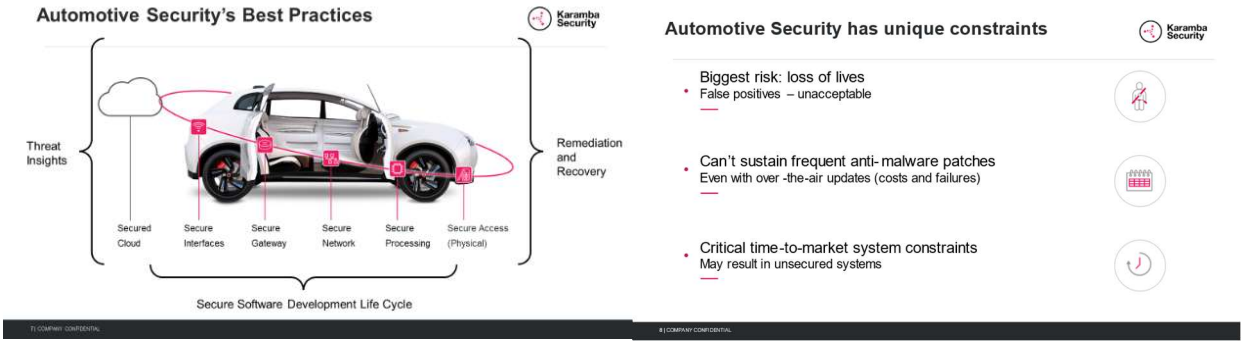
In this design, the TCU can recieve both WiFi and 3G/4G LTE/5G signals. The TCU is capable of a range of functionality including:

- Vehicle-to-cloud (V2X) communication
- Vehicle-to-vehicle (V2V) / vehicle-to-infrastructure (V2I) communication
- Vehicle fleet management and maintenance
- Roadside assistance
- Emergency call (eCall)
- Consumer device integration
- Secured onboard communication

The Gateway ECU and onboard memory provides for storage of related cybersecurity software and firmware (compiled software as “object code”). Messages are received and verified as legitimate (authenticated) by the TCU, prior to release to the Car Area Network (CAN Bus) and into vehicle operating systems.

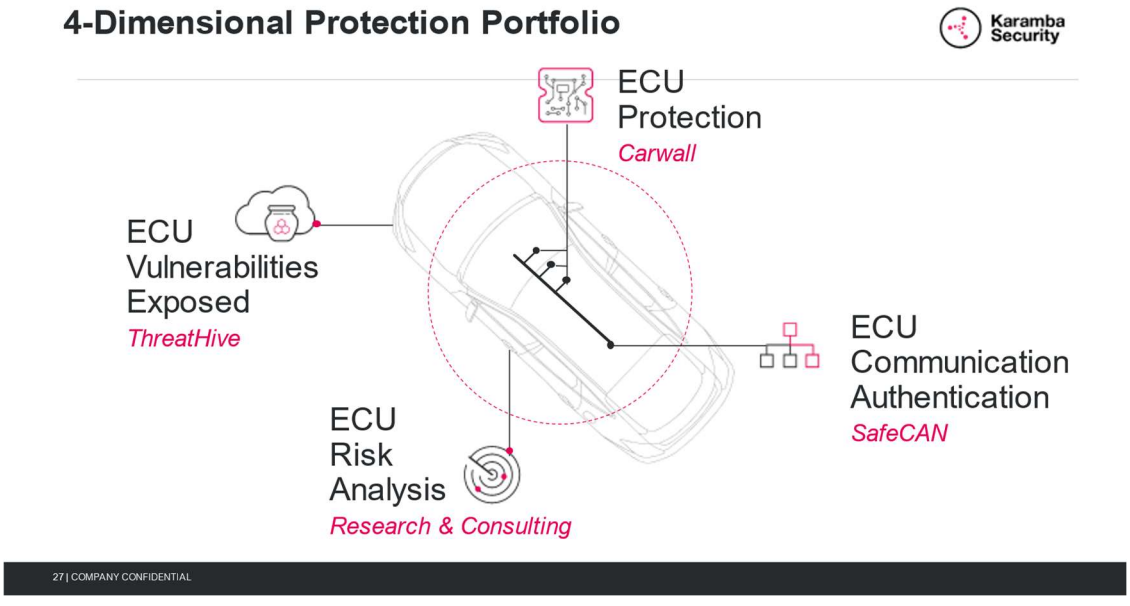
Memory Separation - Over the Air Updates (OTA)

OTA updates for vehicle software have potential for keeping software current for vehicles systems throughout the vehicle’s operating life. With OTA connectivity comes risk if the new code is manipulated by hackers, or non-authorized software updates are made OTA. For this reason, some Tier 1 hardware producers provide separate memory to isolate incoming software updates received OTA. New code is authenticated and evaluated for functional integrity. After this qualification in secure vehicle CPU memory, the updated code is introduced into vehicle control systems.



Current solutions from Industry

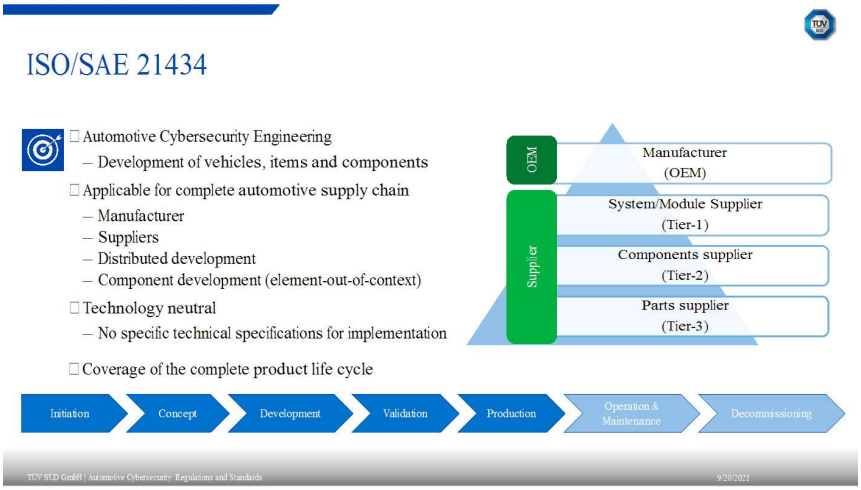
The global supply base for cybersecurity is quickly aligning on wholistic approaches to examine the sources of vehicle systems vulnerability. An example of the various products and services that come from industry include a mix of consulting services and systems licensed for use at the vehicle and OEM levels.



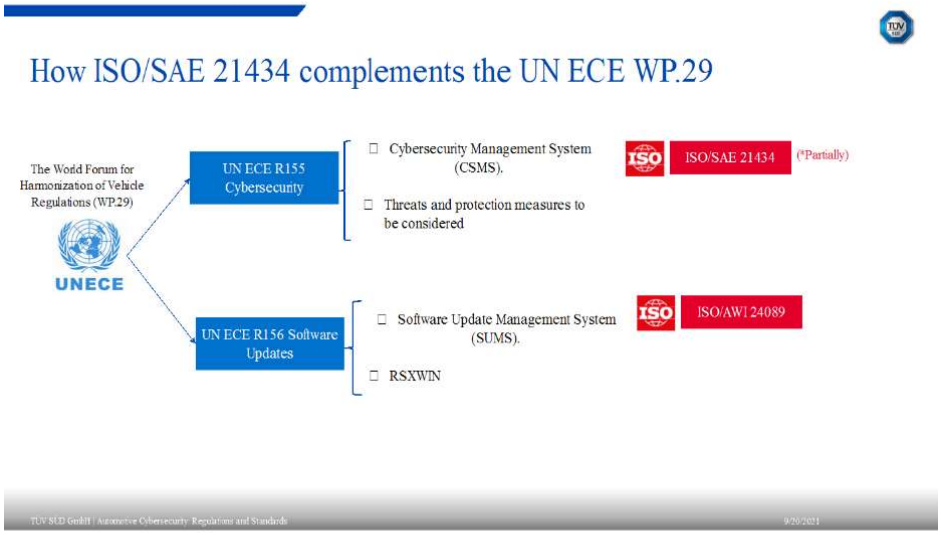
One persistent challenge for cybersecurity services providers is the need to update deployed systems as new threats are identified. This task is daunting and needs to be engineered into systems as the vehicles are designed. OTA holds great promise as a safe and reliable means of making these ongoing updates.

Automotive Industry and National Standards

In the auto industry various standards bodies exist and generate standards promoting safety and vehicle interoperability. Because of the complex nature of cybersecurity and the numerous avenues of attack for hackers, standards groups such as ISO, SAE International, CATARC, and others have promoted a series of recommendations that take the form of best practices. ISO and the Society of Automotive Engineers (SAE) cooperated on a joint recommendation published as ISO/SAE 21434. It was created with a full view of the vehicle operating life from development, components and systems supply, assembly and ownership experience, as summarized here:



The standard was created to dovetail this effort into similar cybersecurity requirements generated by the United Nations Economic Development Council Europe, organized under an effort known as WP.29. WP.29 was organized by the EU, UK, Japan, and South Korea to harmonize vehicle regulations in the markets they serve. WP.29 issued two related regulations supporting the topic of vehicle cybersecurity: UN ECE R115/6, governing cybersecurity and software updates in vehicle applications. As written, both the WP.29 and UN ECE regulations align and complete the risk management for vehicles.



One of the WP.29-based regulations was a requirement that vehicle OEMs demonstrate compliance to its standards for individual vehicles and, following audit, receive certification for specific models.

Work Remaining and Areas for Innovation:

Systems to identify code vulnerabilities will need to be continuously updated as new worms, bots, viruses, and trojans are discovered and mitigated. Automotive industry cybersecurity best practices from (WP.29 7.2.2 – Annex 5) require ongoing sharing of threats to the broader automotive community as new issues are identified. Making this sharing seamless and global seems an area for additional efforts. Identifying new threats and creating effective systems to detect, quarantine, and disable bots, worms, and their many close relatives will keep software experts very busy in the future.

The Role of IP and the Role of the IP Profession in Market Adoption

IP in the form of software and compiled code (firmware) forms the basis for much of the automotive cybersecurity products being deployed today. This software resides in essentially all areas supporting connected vehicles, including the vehicle systems themselves, in the cloud, and in OEM servers tracking a variety of vehicle owner support systems like OnStar, Audi Connect Care, Toyota Connected Services, and BMW ConnectedDrive. This software code is generally proprietary and little of the standards work by world engineering and governmental groups is likely to change that proprietary ownership status. Standards for cybersecurity focus mainly on best practice for vehicle development and incident evaluation and sharing within the industry. These best practices don't rely on standard hardware or interface software or protocols, that in other applications drive the need for FRAND licensing of standards-essential patents. Software used to encrypt and validate message authenticity is broadly available in the market under license.

Several of the recommended best practices (NHTSA Cybersecurity Best Practices for the Safety of Modern Vehicles sec. 4.2.6; AUTO-ISAC Automotive Cybersecurity Best Practices 4.3.3) suggest the creation of a software Bill of Materials (BOM) for all vehicle software in use for each ECU. This software BOM serves as a formal record of the source of all code active in vehicle systems. The software BOM can also provide a record of the use of code developed and made available under open-source licenses. Helping clients understand this important link to code and rights shared under open-source licenses offers the IP profession the opportunity work with the customer engineering community to create a permanent link to code and IP rights received and granted. Being aware of the recommended best practices (included in the annex), presents an important basic step for IP professionals working with software development and licensing.

Hardware, complete with firmware (compiled software) at key entry points for vehicle communications, such as TCUs likely will remain proprietary IP. The IP profession will continue to play an important role in securing patents and software protection in various forms to these elements of design for clients in world markets and supporting licensing activities for these rights to third parties.

In Conclusion

V2X and increasingly "connected vehicles" represent an important step forward for user safety, comfort, and convenience. OTA updates provide a major improvement to enable vehicle manufacturers to refresh software, to react to improved functionality, and to eliminate vulnerability to known software defects. Making sure that these new links to the vehicle are safe and secure will require a lot of great software and vehicle systems hardware designs, and thus, IP forms the basis for creating unique value in world markets.

John Carney

Chair – Automotive Industry Advisory Board
Licensing Executive Society International
john@chinaipxchange.com
1-248-561-4795

Special thanks for presenters for our session and their contributions (right click to open the embedded file)

Karamba Security
Ami Dotan Co-Founder & CEO
ami.dotan@karambasecurity.com


Karamba Security -
The State Of Autom

TÜV SÜD
Johana Constante Perez - Cybersecurity specialist
johana.constanteperez@tuvsud.com


TUV-SUD_Regulatio
n.pdf

Shihui Partners
Sylvia Liu – Of Counsel
liuxx@shihuilaw.com


China Cyber
Security Shi Hui Part

Other Reading and References (links)

Vehicle Cybersecurity | NHTSA

Cybersecurity Framework | NIST - Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 National Institute of Standards and Technology April 16, 2018: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Cybersecurity Best Practices for the Safety of Modern Vehicles (nhtsa.gov)

NHTSA - vehicle_cybersecurit

WP29 – UNECE Cybersecurity and Software Outline (extracted from BlackBerry Website)

WP%2029%20-%20 UNECE%20Cybersec

Auto-ISAC, available at: https://automotiveisac.com/best-practices/download-best-practice-guides/