Advancing the Connected Vehicle

Automotive Megatrends USA 2015

Scott J. McCormick, President
Connected Vehicle Trade Association
Evolution to Autonomous Vehicles

Connected
- Mobile Communications
- Instant Asset Tracking
- Real Time Traffic Info
- Electronic Tolling

Coordinated
- Coordinated Routing
- Optimized Traffic Flow

Cooperative
- Cooperative Collision Avoidance
- Transit-aware Signal Preemption
In-vehicle data and system security
In-vehicle data and system security

• Opening any communication gateway incurs risk of data corruption, loss and system failure from malicious intent, software collisions and bad programming.

• There are up to 15 different frequencies and wireless services on today’s cars:
  • AM/FM, TV, Digital Audio Broadcasting, Remote Keyless Entry, Tire Pressure Monitoring, cellular phone, WiFi, satellite navigation (GPS) and satellite radio, Bluetooth, DSRC and Radar.
  • These systems operate on many different frequencies: 1 MHz, 100 MHz, 315 - 2100 MHz, 1.575 GHz, 2.3 and 2.4 GHZ, 5.9 GHz, 24 and 77 GHz.

• As more access is provided to wirelessly send and receive road, weather and traffic information, as well as infotainment content, more risk is incurred.
Automotive Electronic Control and Communications Safety Systems

- Electronic Stability Control
- Electric Power Steering
- Lane Departure Prevention
- Automatic Parking
- Automatic Steering
- Forward Crash Mitigation – Automatic Braking
- Adaptive Cruise Control
- Engine Control
- Electronic Throttle Control
- Active Suspension
- Antilock Braking
- Regenerative Braking
- Battery Safety Management
- Hill-Hold Control
- Dedicated Short-Range and Voice/Data Communications
- Automatic Start/Stop
Primary Components of Connected Vehicle Communications

• The communication links between the car and the outside world (Radio, Cellular, GPS, WiFi, DSRC and Bluetooth).
• The in-vehicle CAN networks that carry all the vehicle’s operational signals.
• The information and entertainment networks that now carry music, video and voice, and will be the repository of apps, personal data and other content.
Vehicle Vulnerabilities

• Researchers and hackers have penetrated, modified, corrupted or taken control of vehicle systems through the following:
  • Wireless Tire Pressure Monitoring System
  • In-vehicle WiFi (802.11 b/g/n)
  • In-vehicle cellular phones
  • CD Players and infotainment systems

• Vehicle Safety Messages transmitted via Dedicated Short Range Communications (DSRC at 5.9 GHz) are the most secure and will be used for (Vehicle to Vehicle (V2V) and some (Vehicle to Infrastructure (V2I) communications.
Addressing Security

- Threats exist to identity, confidentiality, data and application integrity, intrusion for malicious intent, and disrupting continuity of service.
- In-vehicle software can have up to 100 million lines of code which executes on both the primary computer board(s) and 70-100 microprocessor-based electronic control units (ECUs) networked throughout the body of the car.
- Threats exist from both bad programming and the inability to test all possible software interactions.
- A large number of vehicles communicating to each other is essentially an ad-hoc, self-forming network of devices with no server-side security.
- As vehicle communications are new to automakers, understanding and protecting the systems are a major, ongoing priority.
- As with computers, as the vehicle ages, new threats will surface.
Data Ownership and Privacy
Big Data

- Data can be “Big” not just by volume, but by velocity, variety and value.
- A single car produces an exabyte of data (a billion gigabytes) per year.
- Isolating useful data to extract knowledge from is a monumental task.
- Managing massive data repositories is a huge concern for automakers.
- Trend and cycle assessment of road and traffic conditions, vehicle performance, etc. from timeframes of minutes to years is valuable.
- The next step is to mesh the above data to other knowledge bases in a refine out purchasing relationships, maintenance needs and sales opportunities.
Data Ownership and Privacy

- With the advent of vehicle systems that can receive, store, analyze and transmit data, concerns arise with security and privacy of that data.
- The data you car will hold may include credit card information for tolling systems, personal banking information, work web portal and other credentials, as well as origin/rout/destination for your trips.
- Some vehicles already provide concierge services to a call center, collect diagnostic and vehicle performance data, as well as mileage, and driving behavior.
- Wireless services are forecast to increase substantially, generating more opportunity for transmitting and storing personal data.
In-Vehicle Data

• Almost all of the data a vehicle generates is used by internal systems for engine management, steering and braking, command and control of subsystems, etc.

• Almost all of the data above is proprietary to the carmaker or their suppliers.

• Very little of the data is attributable to your travels, driving behavior or other personal information.

• The raw data is rarely useful, although the derived knowledge can be.

• Isolating useful data to extract knowledge from is a monumental task.

• If automakers or others wish to harvest and analyze that data, it should only be with the permission of the vehicle owner.
Data Ownership Policy Issues

• Automakers differ widely on what data the vehicle owner have rights too.
• Consumers vary even more widely on what information they do or don’t want, or are willing, to share.
• Accessibility to the data is difficult, may void warranties, and is not generally human-readable.
• Should a car owner have rights to ‘see’ car data he doesn’t have rights to (vehicle diagnostics, performance, etc.)?
• Why should my car have a different privacy policy and regulation than my phone or internet connection, cable or marine radio?
Enabling Capability for Existing Vehicles
Enabling Capability for Existing Vehicles

• Approximately 66 million new cars are produced every year worldwide.

• It is estimated that there are over 1 billion cars on the roads.

• The average car in the US is over 11.4 years old, and people are keeping them an average of 11 years.

• If only new cars have advanced communications technology, it will take over 15 years to replace the world’s fleet.

• Enhancing existing cars with communications capabilities increases their value, safety and salability.
Penetration Issue

• Since only 6.7% of the cars on the road are replaced every year, a new car with vehicle to vehicle communications capability would rarely have an opportunity to share road condition, weather, traffic and proximity information for years.

• If we started V2V capability on all new cars today, it would take 7.5 years before just half the vehicles were equipped.

• Aftermarket systems and nomadic device with communication capability could accelerate the benefits not only for cars but for cyclists and pedestrians as well.

• Infrastructure needs can be minimized, but additional investment will be needed.
Aftermarket Opportunities

• Cars without advanced capabilities can have aftermarket systems added for forward collision warning, lane departure, heads-up displays, vehicle-to-vehicle communications, WiFi and Bluetooth.

• The above items would not be integrated into the vehicle control system initially, but as standalone warning and communications systems.

• With automakers opening up their APIs to programmers, it is possible that new aftermarket devices could integrate into the vehicle control architecture, and possibly add more processing power and memory to the car.

• Pairing aftermarket devices with apps on smart phones can add unique capability at a lower cost.
Training and Certification
Collateral Opportunities

• Industries typically outside of the automotive ecosystem are now entering with new business models:
  • Insurance and Repairs
  • Application Development
  • Marketing and Advertising
  • Energy and Grid Management
  • Data Management and Analytics
  • Home/Office/Vehicle information sharing

• With these industries come new data needs, threats, privacy concerns and aftermarket products for existing cars.
The Problem

- The amount of misinformation, misconception, and lack of understanding is growing daily.
- With industry media and advertising reporting on relatively narrow views of some newsworthy aspect of this space, it becomes a monumental task for practitioners and professionals to understand the ecosystem.
- Mainstream media, while getting better at reporting what is going on, often mischaracterize both the purpose and value of the activities.
- To address this problem there needs to be a structured training program that address all of the foundational aspects of the entire ecosystem.
The Connected Vehicle Professional™ Credentialing Program

- The Connected Vehicle Professional™ (CVP) Credentialing Program is a comprehensive education and certification curriculum collaboratively launched between SAE International, Connected Vehicle Trade Association (CVTA) and Mobile Comply.

- Coursework focuses on a combination of hands-on coding and instructor-led lectures. This training style encourages participants to interact with instructors and provides a practical learning environment.

- Business requirements are gathered and defined quickly, enabling the diagnosis of architecture and development problems. The unique team environment and rapid prototyping methodologies deliver better solutions, faster.

- Learners who successfully complete the end-of-course learning assessment are awarded the SAE International/Connected Vehicle Trade Association Certificate of Competency.
Summary

• Vehicle communications must be secure and trusted, and industries and governments are working on this.
• Vehicles will have communication capabilities well before data ownership and privacy policies are finished.
• Vehicle owners should have the right to opt-in to any use of their data, and know how that it will be used.
• A large opportunity exists to enhance existing vehicles with aftermarket systems and nomadic devices such as smartphones, tablets and laptops.
• It is necessary to provide certifiable training across the breadth of the ecosystem.
Scott McCormick
51037 Weston Drive
Plymouth, Michigan USA 48170
Bus: +1.734.354.0546
Fax: +1.734.446.0326
Cell: +1.734.730.8665
Skype: scott.j.mccormick1

sjm@connectedvehicle.org
www.connectedvehicle.org
Scott has degrees in Mechanical and Aerospace Engineering, a Master’s in Business Administration, and Post Graduate Research in Artificial Intelligence. Prior to CVTA, Scott was the first President of the VII Consortium and before that the Executive Director of the AMI-C, a nonprofit research organization of the world’s largest automakers.

Scott is a former Advisor to the US National Science Foundation and the Industry Representative the US Federal Laboratories Technology Transfer Consortium. He is the former Strategic Advisor to the United Nation’s International Telecommunications Union (ITU-T) Advisory Panel on Communication Standards to Vehicles.

In 2012, Scott was appointed by the US Congress to the ITS Program Advisory Committee to advise the Secretary of Transportation and Congress on matters relating to the study, development, and implementation of Intelligent Transportation Systems.
Who We Are: Connected Vehicle Trade Association

• CVTA is an international, non-profit trade association formed to advance the interests of industries and organizations involved in vehicle communications.

• Membership is open to companies, universities, standards bodies and public agencies globally.

• The Board of Directors was established with one representative from each industry involved and includes Delphi, Magneti Marelli, Nokia, Cisco, Intel, Visteon, Verizon, Oracle and Road America, among others.