Perspectives on Vehicle-to-Vehicle Communications

Steven H. Bayless
Vice President, Regulatory Affairs and Public Policy
ITS America

October 18, 2016

www.itsamerica.org

Light Reading Webinar "The Connected Car – Invisible Wireless Threads Linked to an Autonomous Future"
**Long Term Effort:** From 2005, automakers, universities and USDOT work to develop standards to support V2X and conduct proof-of-concept and scaled-up operational tests

**Safety Benefits:** NHTSA proceeds with advanced notice in 2014, citing that Vehicle-to-Vehicle (V2V) could address 80% of unimpaired crashes

**Proposed Standard:** NHTSA to release Proposal to create Federal Motor Vehicle Safety Standard No. 150 (FMVSS 150) – some potential elements

- Require all light vehicles to have V2V communications capability
- Create minimum performance requirements for all V2V devices and messages
- Currently Dedicated Short Range Communications (DSRC) is furthest ahead with enough standards & analysis/testing track record to meet rulemaking requirements

**Industry Consensus:** Autos want to proceed this year, and White House just announced intention to allow NHTSA to move forward with V2V (in coordination with release of Automated Vehicles policy)
The Wireless Access For Vehicular Environments: (WAVE) stack addresses applications, interoperability, privacy, security, media access (SAE, IEEE standards)

Short Range Peer-to-Peer model: V2X equipped vehicles pass messages to only neighboring cars/traffic signals (<300 ft to support “highly local/highly current” apps)

Robust Interference Mitigation: licensed spectrum dedicated for V2X DSRC provides assurance for mission/safety critical operations

Privacy Assurance: Messages are anonymized alerts– no driver, vehicle, or other identity information provided

- Neighboring vehicles and other nodes use anonymous messages to determine if there is a risk of collision for crash avoidance applications
- If crash risk is determined to be high, alert if generated to driver.
- Anonymity efforts assures drivers with V2V cannot be subject to surveillance

Security Assurance:– operational design that addresses potential threats major part of “connected vehicle” effort
ITS America supports Vehicle Safety Communications (V2V) Rule at NHTSA under consideration – Major issues to address:

- **Interoperability** - One standard for all vehicles and all traffic control systems enables industry to focus on new application development without worrying about low level interoperability.

- **Safety/Security/Operational Assurance** – suitability for IOT crash avoidance, driving automation, or intelligent signal control, not broadband/infotainment.

- **Equipage Path** - Voluntary adoption vs. Mandate (or similar accelerated adoption model) – utility of V2X is a function of number of nodes equipped.

- **Vehicle Aftermarket** – will accelerate adoption far more than OEM alone.

- **V2X App Ecosystem** - More app development and ongoing commitment to security, privacy and other foundational assurance elements.

- **Intelligent Infrastructure** – Road Infrastructure operators needs are different from autos/aftermarket, so much more attention for Vehicle-to-Infrastructure apps.