Vehicle-to-Vehicle Communications: Readiness for Application

Daniel C. Smith
Senior Associate Administrator for Vehicle Safety
National Highway Traffic Safety Administration
April 2014
Terminology

• “Terminological inexactitude” (better known as sloppy language) breeds confusion

• What do you mean by “connected” vehicle?
  – Vehicles “connected” to each other, pedestrians, and infrastructure for safety and mobility?
  – Vehicles “connected” to the Internet for general communications, entertainment, etc.?

• Why does it matter?
  – Very different technologies, potential benefits and risks, safety issues
Differing Visions of the Future

• Three streams of innovation
  – V2V, V2I, V2P, V2X
  – Automation
  – Self-driving (autonomous)

• Some are true believers in one stream and naysayers about the others

• Some see possible convergence and others see competing alternatives
NHTSA’S VISION

• Goal: reducing risk of crashes, injuries, and deaths at the fastest reasonable pace through improving technology and driver performance
• Tools: data, research, rulemaking, enforcement
• Preferred technologies: any for which safety effectiveness can be demonstrated, benefits justify costs, public likely to accept
• Desired end state: dramatic reduction in number and severity of crashes and the consequent harm
V2V Research Report

– Safety issues V2V and V2X can address
– NHTSA’s legal authority
– Technical practicability: interoperability, system limitations
– Safety applications: performance metrics
– Security system
– Consumer and industry acceptance; privacy
– Legal liability
– Additional research needs
Safety Need

37 Pre-Crash Scenarios
All Light-Vehicle (LV) Crashes (5,726,000)  Unimpaired LV Crashes (5,355,000)

22 V2V Pre-Crash Scenarios
4,336,000 LV Crashes
(76% of All LV Crashes, 81% of Unimpaired LV Crashes)

17 Target V2V Scenarios
3,662,000 LV Crashes
(64% of All, 68% of Unimpaired)
- 5 Rear-End
- 3 Lane Change
- 2 LTAP/OD (all intersections)
- 2 Traffic Control Device Violation

10 Priority Scenarios
3,224,000 LV Crashes
(56% of All, 60% of Unimpaired)
- 3 Rear-End
- 2 Opposite Direction
- 1 Junction Crossing

5 V2V Pre-Crash Scenarios
12% of All LV Crashes
13% of Unimpaired LV Crashes
Not Used
- 2 Control Loss
- 1 Backing
- 1 Parking
- 1 Other

15 V2I or Single Vehicle Pre-Crash Scenarios
24% of All LV Crashes
19% of Unimpaired LV Crashes
Not Used
Legal Authority

Regulatory Authority

• NHTSA has sufficient legal authority under the Safety Act to regulate on-board V2V equipment (and aftermarket V2V equipment) and related software and to facilitate development of a security system; but not to require the OEMs to stand up an SCMS or to regulate it directly

Agreement/Contract Authority

• A security system needs to exist to ensure that V2V messages are reliable/trustworthy. For this reason, NHTSA has authority to enter into agreements or contracts, either cost or no-cost, to ensure existence of the necessary security services; Note: NHTSA has no funds to establish or operate the system
### Elements of the Safety Act that would Apply to agency action regarding V2V

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance Oriented</strong></td>
<td>Motor vehicle standards define the minimum performance for compliance.</td>
</tr>
<tr>
<td><strong>Meet Motor Vehicle Safety Need</strong></td>
<td>Must be a nexus between the standard and the safety problem</td>
</tr>
<tr>
<td><strong>Objective Standards</strong></td>
<td>Test procedure that are capable of producing identical results when test conditions are exactly duplicated.</td>
</tr>
<tr>
<td><strong>Practicable Standards</strong></td>
<td>The standards must not have technical uncertainties and must be economically feasible in terms of significant costs that may harm a well-establish industry.</td>
</tr>
<tr>
<td><strong>Public Acceptance</strong></td>
<td>Public needs to accept and use correctly.</td>
</tr>
</tbody>
</table>
Technical Practicability
(TEchnological Readiness of V2V)

- Technical Readiness
  - Vehicle Based
  - Non-Vehicle Based
  - Hardware
  - Security
  - Software
  - Interoperability
    - System Limitations
    - Global Coordination
    - GPS Availability
    - Relative Position
    - Message Congestion
    - Device Installation
    - Device Updates
    - Communications
    - Message Sets
    - 5.9 GHz spectrum
    - Standards
    - Performance Measures
    - Safety Applications
    - DSRC
Safety Applications

• Looking at six important ones:
  – Forward collision warning
  – Blind spot warning and lane change warning
  – Do not pass warning
  – Left turn assist
  – Emergency electronic brake lights
  – Intersection movement assist

• Analysis concerns each application’s:
  – Technical maturity—e.g., false warnings
  – Possible performance metrics, driver-vehicle interface
Public and industry acceptance

• Public:
  – Privacy
  – Confidence in the technology
  – Cost
  – Convenience (e.g., new security certificates)

• Industry
  – OEMs concerned about interacting with vehicles or aftermarket equipment they did not produce
  – Public reaction, especially privacy issues
  – Cost
  – Relationship to on-board technologies
Security

Security Credential Management Systems Technical Design

- Technical Requirements
  - Establish trusted environment
  - Secure against internal and external threats and attacks
  - Support V2V safety messages using DSRC
  - Support NHTSA mission-based informational needs
  - Appropriately protect privacy

Legend:
- Regular Communication
- Out-of-band Communication
- Initial Deployment
- Full Deployment
- Find in Every PKI
- Typical in PKI
- Unique to SCMS
Remaining Issues

• Additional research needs such as
  – Performance standards for DSRC devices
  – Performance metrics for safety applications
  – System security
  – Mitigating communications congestion
• Spectrum: to share or not to share
• Security system: who will operate?
Next Steps

• Issue the research report with request for comments
• Issue a request for expressions of interest in establishing and running the security system
• Complete research needed for proposed rule
• Draft proposed rule and submit for executive branch review, including full analysis of costs and benefits
• Detailed privacy risk assessment and security review