Operations Opportunities and Technology Challenges-

Tom Schaffnit
A2 Technology Management LLC

Current DSRC Technology

- Lower layers are consistent with current generation Wi-Fi technology
- V2V safety technical requirements are most stringent
- 10 MHz channelization proven through years of field testing (automobile industry in cooperation with USDOT)
- Channel 172 for V2V safety also proven through extensive field testing
- Most relevant standards are now in place – stable technology foundation

Challenges to a Coordinated Nationwide Deployment

- Interoperability:
  - Possibility of V2I regional & local variations
  - V2V & V2I requirements harmonization (esp. security)
  - Process to facilitate infrastructure-related applications installation in vehicles
  - Mandated functions vs opt-in applications
- Deployment timing:
  - Security communications and backend to support V2V functions
  - Mandated vehicle deployment, but lengthy fleet penetration
  - Nationwide coordination of infrastructure deployment
- Customer acceptance:
  - Perception of value
  - Protection of personal information
  - Effective public messaging

DSRC Spectrum Protection

- DSRC spectrum protection is a major issue for Connected Vehicle program
- Major societal push for more free broadband Wi-Fi spectrum
- Historical FCC role – protect incumbents from "harmful interference"
- Spectrum analyzer scan currently indicates "vacant spectrum" at 5.850 – 5.925 GHz
- Crash imminent safety – both V2V and V2I – may only be able to justify 2 – 3 DSRC channels
- Envisioned infrastructure applications need more definition, more definite deployment plans and strong advocacy with FCC

Security System as Trust Anchor for V2V and V2I/I2V Functions

- Need for consistent trust anchor (via security system) throughout:
  - United States
  - Likely range of vehicle-based travel (e.g., NAFTA zone)
- Separating the core security systems for vehicles and infrastructure would likely result in:
  - Challenges to interoperability
  - Diverging security technologies and protocols
  - Reduced benefits to end users
- Implementing the same trust anchor for vehicles and infrastructure enables:
  - Transparent support for interoperability
  - Cohesive security policies
  - Ease of developing and deploying applications
  - Enhanced opportunities for creating customer value

Related Cyber Security Issues

- Connected Vehicle systems:
  - Offer major potential safety benefits
  - Likely a foundational capability for self-driving vehicles
  - Introduce additional wireless interfaces to vehicles
- Wireless interfaces potentially introduce new remote attack vectors
- Difficult to implement effective firewalls that allow wireless access to critical systems and also prevent unauthorized access
- Even if system compromise cannot result in serious safety issues, user acceptance is susceptible to widely-publicized successful 'hacking'

Potential for Entrepreneurial Opportunities

- DSRC appears to provide similar opportunities to other long-term technology systems (e.g., GPS, Internet) that have enabled large-scale commercial innovation
- The core system, including security, should provide maximum flexibility for these types of commercial and proprietary innovations, without compromising safety
- Expect the development of a wide-spread ecosystem of commercial applications enhancing customer value

Thank You!

A2 Technology Management LLC

Contact:
Tom Schaffnit
tom@schaffnit.com