A **connected car** is a car linked to something via a defined wireless communications link.
Connected Car
A couple more notes…

An autonomous car is not necessarily a connected car

An autonomous car is not necessarily a driverless car
The world of Vehicle-to-Everything (V2X)
The world of Vehicle-to-Everything (V2X)
V2X = V2I + V2V

Vehicle-to-Infrastructure (V2I)

Vehicle-to-Vehicle (V2V)
Why V2X?
Some examples

**Improved Safety**
- Red light violation
- Severe weather warning
- Road works ahead
- Forward collision warning
- Pedestrian crossing
- Emergency vehicle approaching

**Energy Efficiency**
- Eco driving
- Traffic light priority
- Slow traffic ahead warning
- Vehicle platooning

**Driver Comfort**
- WiFi provision
- Autonomous parking
- Insurance pricing
- Route guidance
Wireless communications

Cellular

- Cellular connection (GPRS, 3G, 4G) is established via devices such as smart phones or in-vehicle cellular equipment
- Better suited for driver comfort applications, where latency is not an issue
- Mobile phone integration augments functionality
- Examples of connected car systems already exist in the market (e.g. Waze)
Wireless communications
Dedicated Short-Range Communication (DSRC)

- Makes use of a special type of WiFi (802.11p), creating a localised wireless network
  - V2V: vehicles are fitted with DSRC transmitter and receiver
  - V2I: infrastructure & vehicles are fitted with DSRC equipment
- Best suited for high speed applications (safety and energy efficient) due to low latency
- Siemens are involved in a number of research & demonstration projects to prove DSRC with V2I
Conclusions

- **Connected cars** already exist, with varying levels of connectivity and different communications technologies.

- **Cellular** communications are more suitable for driver comfort & convenience.

- **DSRC** communications are more suitable for safety & energy efficient applications.

- Connected cars are likely to make use of both cellular and DSRC, depending on the **use case**.
Q & A

Questions?
Thank you for your time!

Priscilla Boyd
Product Manager

Siemens plc
Sopers Lane
Poole BH17 7ER
United Kingdom

Tel.: +44 1202 846005
Fax: +44 1202 782435
Mobile: +44 7808 823736

priscilla.boyd@siemens.com
Securing the Connected Corridor

Andrew Ashby
Plextek Consulting
Consider the broader challenge

Well recognised by multiple industries:

- Widespread recognition of security threat to entire connected vehicle infrastructure - not just to vehicles
- Far less agreement on real-world solutions to protect against them, but a very pressing need to respond
- An expanding attack surface / Rapidly growing threat profile
- Independent thinking needed - recognise overall challenge of who and what to bring together
- How to enable cross sector industry knowledge to deliver secure V2V & V2I connectivity?
Securing the ‘Connected Corridor’

Connected corridors will converge industries, participate in transforming transport implementation, ownership and transport business models.

- Security is the biggest barrier to ‘acceptable’ connectivity
- Secure communications is key to fully integrated services
- Secure data access is the key to value extraction
What needs securing? V2i

- **V2i - Personal**
  1) Online purchasing smartphone to vendor

- **V2i - Car**
  1) Purchasing from Android terminal in car eg
     - Road tolls
     - Car rental
  2) Telematics data – used for
     - Real time vehicle insurance
     - Accident notification and investigation
     - Fraud prevention
  3) Vehicle assistance
     - Find parking spaces
     - Organise traffic flow
V2i – Relationship Example

- V2i Android terminal in car – real time insurance

  TRUST

  verify I am the driver and I will pay for the insurance

  Will not allow the car to start unless a valid driver is present and the insurance is paid

  TRUST

  direct line

  Provide valid insurance

  Check insurance is OK on the road

  AESIN
  AUTOMOTIVE ELECTRONICS INNOVATION
What needs securing?  V2V

- **V2V**
  1) Driver information
     - Cascaded video – reason for queue
  2) Vehicle safety assistance
     - Braking assistance
     - Erratic vehicle warning
  3) Platoon control
     - Real time vehicle control
     - Maintenance of vehicle Platoons
     - Joining/leaving Platoon
V2V – Relationship Example

• V2V Platooning Demonstration

I trust the Platooning System

Each car has compatible systems which are functioning correctly

Role is to ensure legislation supports the required level of safety for society as a whole

• Government
• Regulator
• Public
Scope for a ‘Connected Corridor’ demonstrator

- A primary objective would be a Highways demonstration of real-time connectivity
- Might not expect to apply end-to-end security or ‘chain of trust’
- An opportunity to study one or two implementations of secure connectivity
- A trial exercise of authenticated communications over an existing standard e.g. 4G/LTE
Needs for real world connected corridor

Who?
• All parties with an interest in secure, attack resilient connected corridor functionality, services and business models

What?
• Identify the extent & types of threat across the complete connectivity landscape
• Cross-sector Industry parties need to categorise and quantify the threats
• With relevant parties engaged, support industry (& standards) to drive long term integrated approach to connected corridor
  • with security as a feature from the ground up
  • with test strategies in mind for the connected corridor systems
The Interested Parties

There are many interested parties to: Make aware / participate / legislate:

- Highways England, Service Operators, Infrastructure Providers, Cloud actors
- OEMs, T1s, Innovators, IT solutions, Technology suppliers, T/E providers
- Gov't legislators, Law enforcement, Counter-Terrorism
- Insurance companies, Lawyers
Thank you for your attention

Andrew Ashby
Automotive & Transport Business Manager
Plextek Consulting

andrew.ashby@plextek.com
+44 7840 20928
+44 1799 533237