



Financing Communication Infrastructures for Co-operative Safety Systems

ITS Aalborg, 2007-09-16

**Hans Lind, Elisabeth Uhlemann, & Lars-Göran Rosengren
Volvo Technology**

Who Will Pay?

This Question May Have Two Answers!

Scenario 1:

- Making existing and emerging autonomous safety functions co-operative
- Warnings are transmitted peer-to-peer to enhance situation awareness

Answer 1:

- **Road authorities**
- **Insurance companies**
- **Vehicle manufacturers**

Scenario 2:

- Including new safety functions in existing and emerging co-operative systems built for other purposes
- Warnings are generated locally based on shared total situation awareness

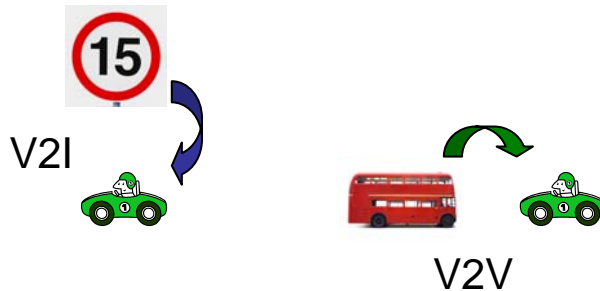
Answer 2:

- **Telecom providers**
- **Road users**
- **Service providers**

Extending Today's Base Cases

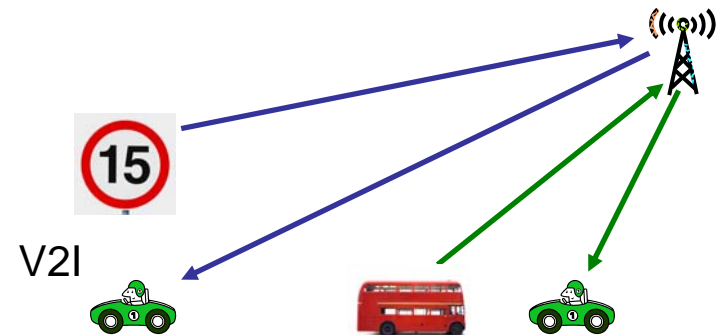
Autonomous Safety Systems Made Co-operative:

- Collision Warning, Blind Spot Detection, ...
- Current technology: Radar, Lidar, ...
- **Future: Co-operative systems: WLAN 802.11p, peer to peer**



Infrastructure Based Co-operative Safety Systems:

- Emergency Call, Traffic Info incl. Warnings, ..
- Current technology: 2G cellular systems
- **Future: Co-operative systems 3GPP LTE, access point**



Market Drivers for Cooperative Safety

Scenario 1: Peer-to-Peer

- Customer demand/incentives:
 - Reduced tax, insurance, or parking costs
 - Improved safety

- Legislation/Regulation
 - Improved safety
 - Road tolling
 - Vehicle maintenance

Scenario 2: Via Access Point

- Customer demand/incentives:
 - Bundling safety to other services, e.g. Norwich Union's "Pay As You Drive" to reduce cost, or separate driving lane
 - Service platforms: enabling advanced services, also from 3rd parties

- Legislation/Regulation:
 - Improved safety
 - Sustainable development (CO₂/NO_x monitoring/taxation)

Scenario 1: Making Existing Autonomous Safety Applications Co-operative

Step 1:

- Many of the suggested applications for CSS can be implemented without co-operation (using sensors): Front collision warning, Blind spot detection
- Some applications already exist together with an on-board user interface

Step 2:

- Next these systems are **enhanced** by communication with a RSU: Front collision warning enhanced by information from traffic signs.
- RSU are then only needed in selected places

Step 3:

- Include vehicle-to-vehicle communications: Blind spot detection enhanced by information from the other vehicle (e.g., weight, bumper height, number of passengers, hazardous goods), hazards ahead on the road, etc
- For equipped vehicles, traffic light information in a crossing is still helpful even if not all non-equipped vehicles running a red light are detected.
- For non-equipped vehicles the pure sensor systems still exist.

Implications of Scenario 1

Technical realization:

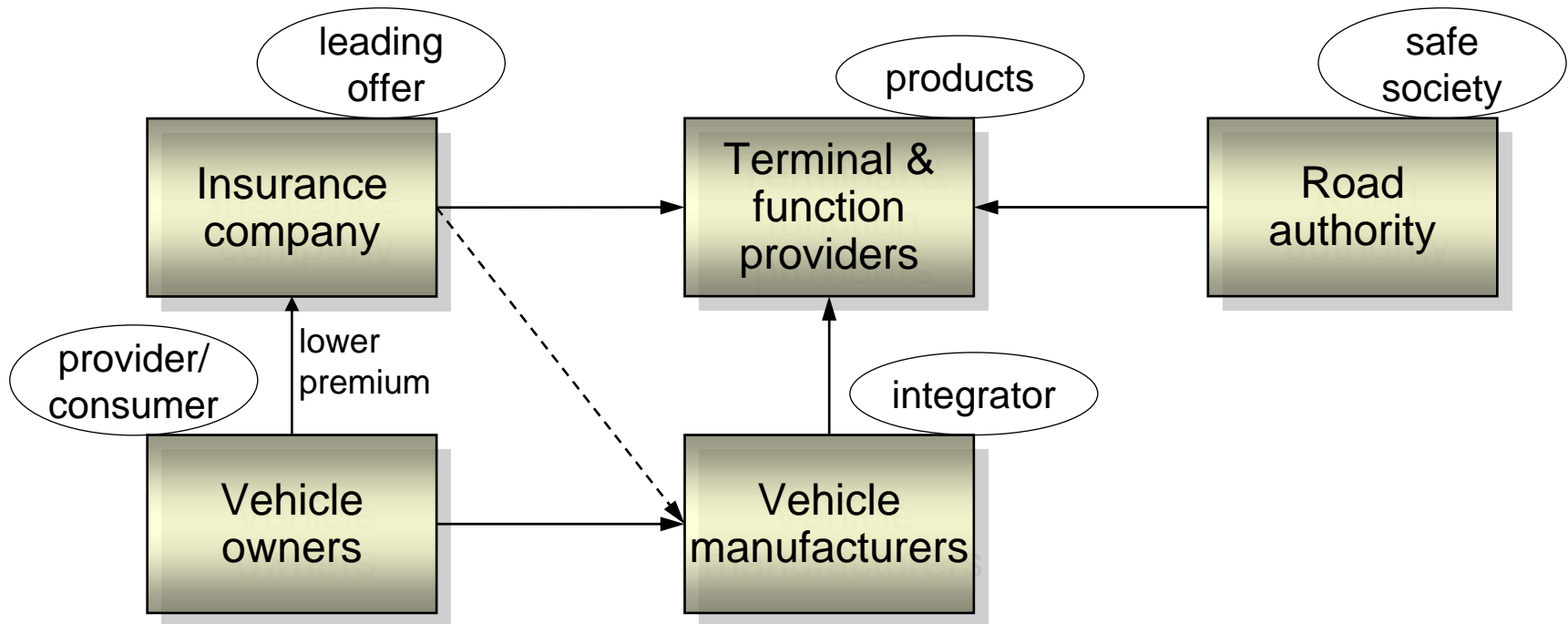
- Short warning messages are transmitted locally in case of incidents
- 100% penetration not required
- Frequency spectrum sufficient – only local sporadic communication
- Communication directly, peer-to-peer (P2P)
- RSU is also a peer
- WLAN units in P2P mode can be used: Low delay, Cheep (no cost for data traffic and low cost for OBU), No additional infrastructure is necessary

Who pays?

- **Road authorities** and **insurance companies** can make and evaluate their possible cost savings by installing RSU in hazardous areas.
- The OBU could also be used for e.g., electronic toll collection or vehicle maintenance and thus **road authorities** and **vehicle manufacturers** may pay for it.
- Governance function operated by **road authorities**

Revenue streams between principal actors

Scenario 1: Communication Direct Peer-to-Peer



Scenario 2: Including safety applications in emerging co-operative systems

Step 1:

- Many projects deal with co-operative systems (FP6 and FP7), e.g. eCall (eSafety Initiative), emergency phone call, CVIS (IP) architecture for co-operative mobility applications, Coopers (IP) co-operative traffic management, Sevecom (IP) security applications

Step 2:

- Next, cooperating units, targeting mainly non-safety applications, may be built into every vehicle.
- RSU are then existing since typically cellular systems are used.
- Vehicle-to-vehicle communication is made via an access point.
- Some safety applications which tolerate a longer delay can be built into these systems too.

Step 3:

- Cooperative monitoring and information fusion from periodic updates can be used to (locally) predict a hazardous incident, i.e. the need for low delay communication is reduced. Blind spot alert may be needed in 10 seconds if all vehicles maintain the same speed.

Implications of Scenario 2

Technical realization:

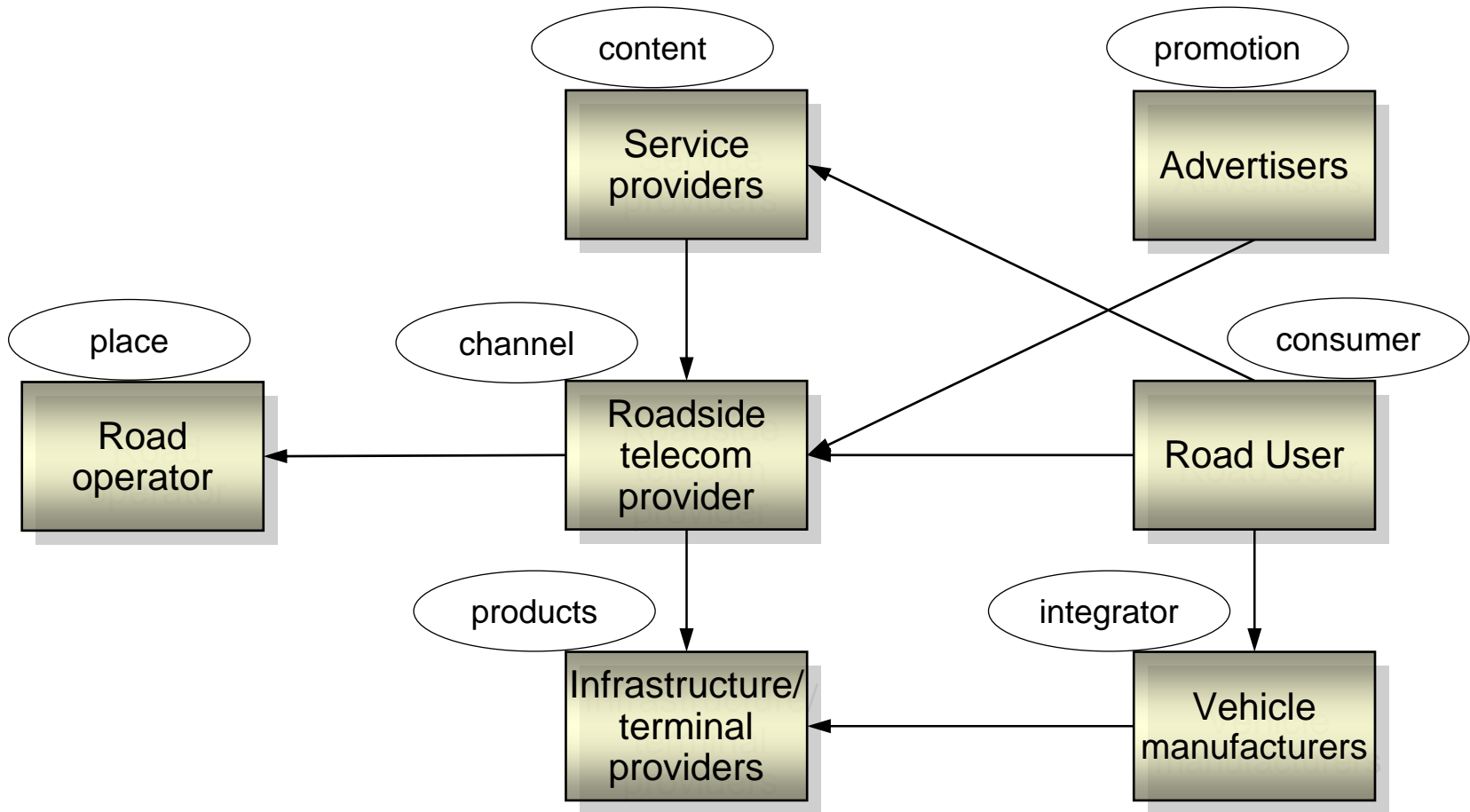
- Information fusion from periodic updates is used to generate warning messages locally
- Close to 100% penetration needed
- Frequency spectrum sufficient – periodic messages over mobile broadband (3GPP)
- Communication via access point (AP)
- RSU is either an AP itself or a peer communicating via an AP
- Existing APs in cellular phone systems can be used:
 - High bandwidth
 - Bundling with existing applications
 - Infrastructure exists

Who pays?

- RSUs could be telecom APs and thus **telecom providers** may pay.
- The OBU could be used for e.g., comfort application or CO2 /NOX monitoring and thus **road users** and **private/public service providers** may pay.

Revenue Streams between Principal Actors

Scenario 2: Communication via Access Point



Keys to Success

- Each technology has its own business model – and answers the question “Who will pay?” in different ways.
- Incentives/legislation supporting customers to buy and use safety critical solutions must be put in place.
- All identified stakeholders need to be involved in the design of future CSS – not only vehicle manufacturers.
- A combination of peer-to-peer and infrastructure based systems brings the best of both worlds.
- Trust and information security are major concerns, e.g.: authentication, authorization, integrity, confidentiality and non-repudiation, that needs to be solved to pave the way for future success.

Back Up

Concerns

Lack of trust

- If you can control a car in good intentions, so will hackers or even terrorists

Personal integrity

- People may find out where you are, if you are speeding, or other data that you are unwilling to share

Initial coverage

- Service availability, reliability and quality

Service diversity, price and attractiveness

- Economies of scale, business models and service distribution



Question by the Conference Organizer

Future safety systems

- Today's cars and trucks are safer than ever. More and more features are included as standard, and advanced driver assistance systems are appearing across all model ranges. The future will depend on cooperative safety systems based on mobile vehicle communications.

But who will pay for this new communication network infrastructure and for the accompanying investment in “talking” interfaces to roadside infrastructure?

- Another challenge is how to make sure that advanced driver safety products/services are so attractive that they become part of the “must have” option pack that every driver chooses!