

SAFESPOT Use Case Speed Alert

Klaan van Wees

SAFESPOT BLADE

k.vanwees@rechten.vu.nl

Vrije Universiteit Amsterdam, subcontractor TNO

December 2, 2009

Joint eSecurity WG / Article 29WG meeting

Speed Alert

The Speed Alert application aims at providing a recommended speed to drivers on the basis of real-time evaluation of parameters such as: the weather status, road surface conditions, topology of the road, traffic flow speed and any events like road works, traffic jams, and deviations.

Context

Main objectives of SAFESPOT

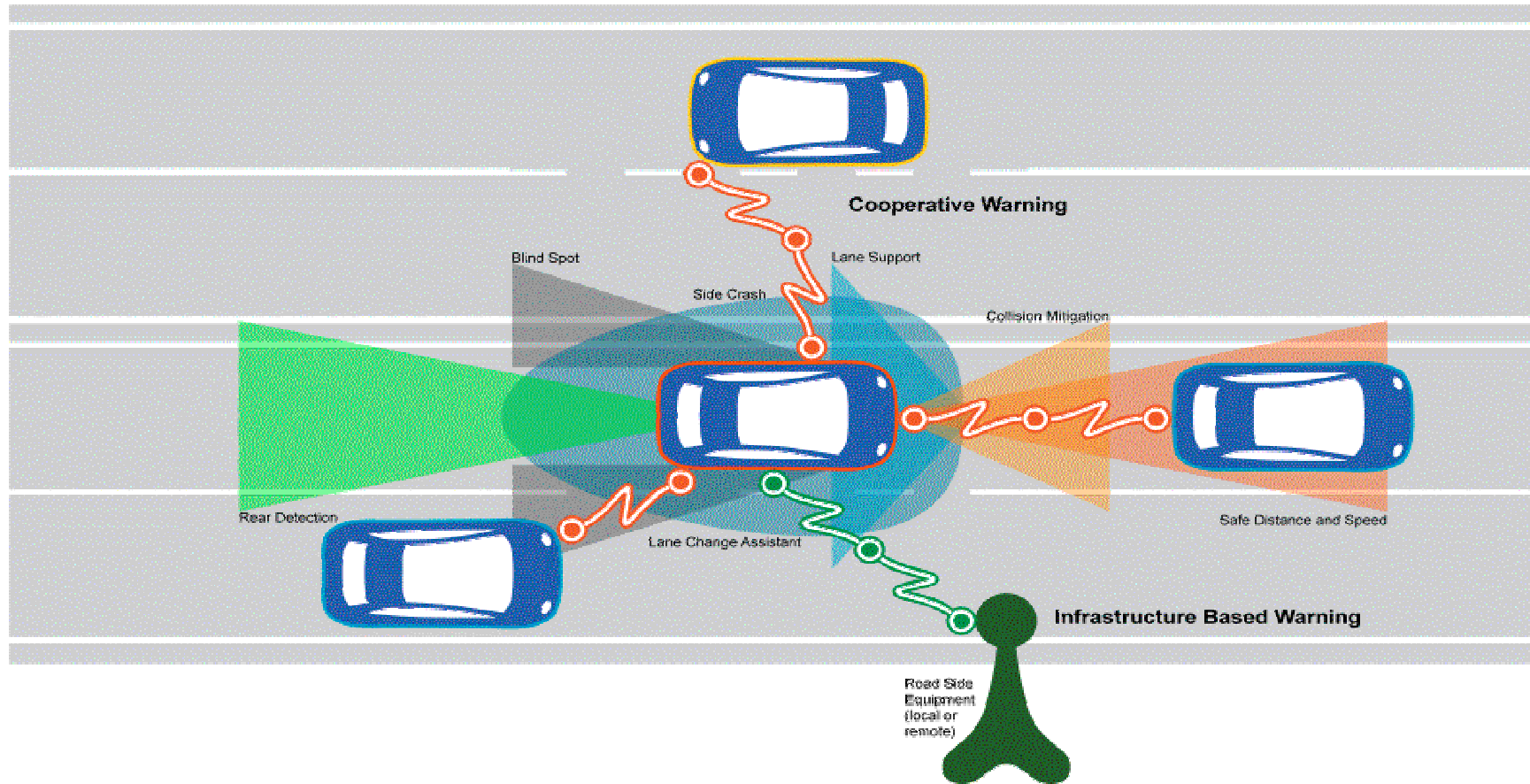
- To develop or improve and assess the key enabling technologies
- To develop the Safety Margin Assistant (integrated application framework using the safety-related information provided by the network properly fused with the on board sensors and able to advise the driver in order to keep the vehicle as possible from emergency situations or to provide a proper warning when they occur)
- To define in common with other EC-projects an open, flexible and modular architecture

Context

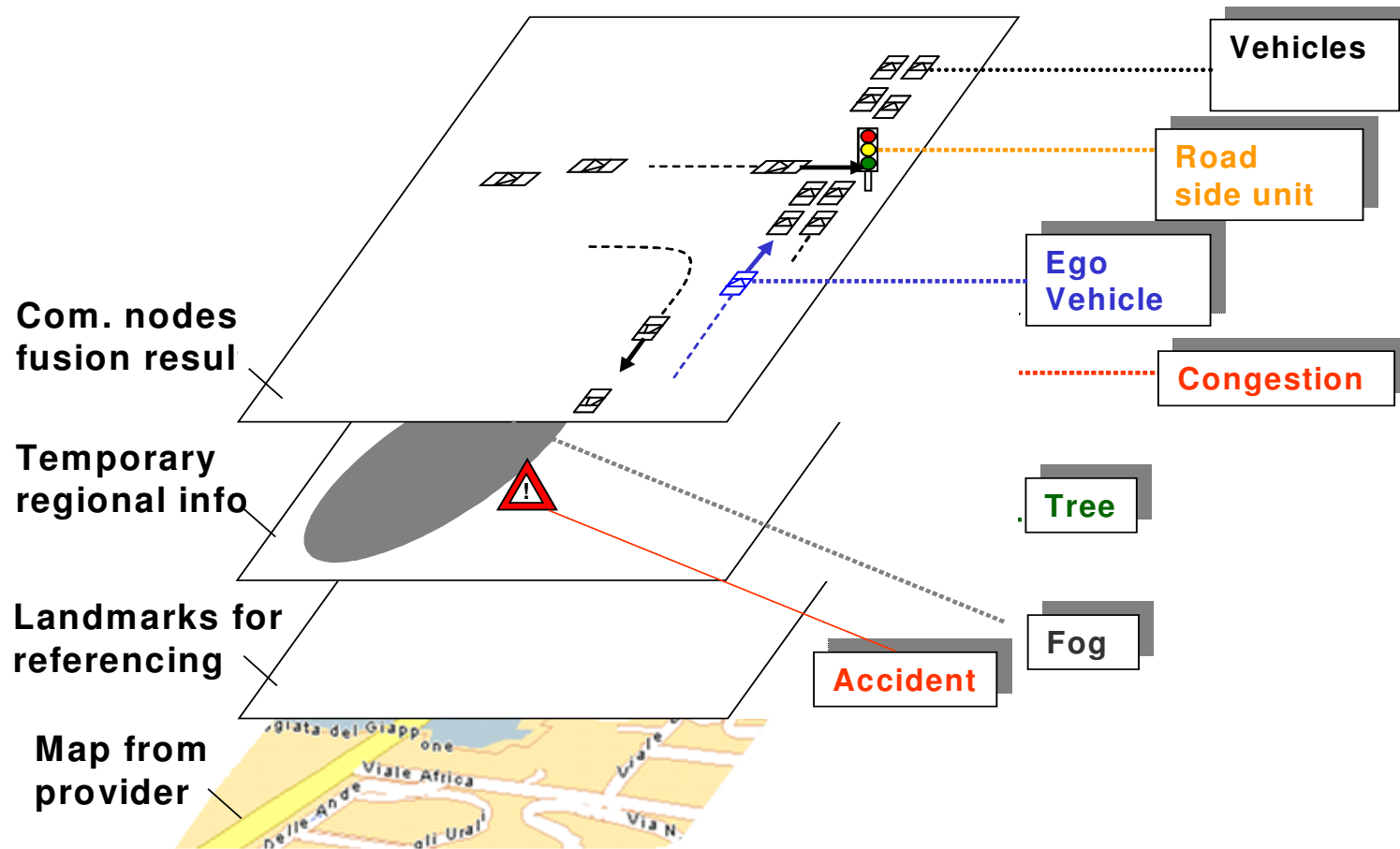
SAFESPOT architecture

- System is composed of a set of “nodes” (equipped vehicles or RSUs)
- Able to exchange information through short range wireless communication (IEEE802.11p.) called the VANET (Vehicle Ad-hoc Network) and to use this information in order to generate messages for the drivers
- A node runs applications using data provided by other nodes and/or by its own sensors
- Available data are collected in a multilayered Data Base named Local Dynamic Map (LDM)

SAFESPOT warning scenario



Local Dynamic Map



Messages, Storage and Access

Probe vehicles to RSU/other probe vehicles

- (fixed) Vehicle identifier for tracking on the LDM and the classification of generic type of a vehicle, which can be helpful for other sub applications or for special legal speed limit (alternatively vehicle identifier may be assigned by receiving equipment)
- Vehicle status data (location, speed, etc.)
- The vehicle path planning data (if the driver has set a given path on his vehicle navigation system) could be used in order to filter for possible problems.

Messages, Storage and Access

RSU to Probe Vehicles

- Data other probe vehicles
- Data other road users (location, speed, etc., gathered through infrastructure sensors or data communication)
- Dynamic information on road status and road geometry
- Speed limits

Messages, Storage and Access

- Data flows and processing in a VANET (ad-hoc network) for SAFESPOT purposes: data are being processed on the LDM but are not stored for longer periods (they are only processed/ stored as long as they are within the local geographical scope of the vehicle LDM)
- SAFESPOT applications as such do not require centralized storage of data

Data protection issues: Who is the data controller/processor?

- Ad hoc nature (VANET) of SAFESPOT applications
- No central Controller (VANET is a network of nodes)
- Who is the data controller?
 - > Who determines alone or jointly the purposes and means of the processing of personal data within the context of SAFESPOT applications
 - Car/system manufacturer?
 - Infra operator?
 - If bundled -> (also) service providers

Data protection issues:

1) Need to clarify the role of ITS actors

- This is ongoing research within Safespot: WP 6.3 (Organisational Architecture) and WP 6.6 (business models)
- Within WP6.3 four types of 'exchanges' were identified:
 - Operational data (real-time info/ periodically updated content)
 - Services
 - Licenses/ Authorizations/ Certificates
 - Rules
 - HW and SW products

2) Need to determine the legal basis on which ITS services will be provided (e.g. mandatory)

- Deployment scenario's that are being taken into account include both public (including mandatory) and private driven (voluntary/marker) deployment paths
- Legal basis requirements depends on deployment scenario

3) Need to take into account the notion of anonymous data in it's very strict definition under the data protection law

- ?????

Data protection issues:

4) Need to determine the purpose of data processing when it takes place (operation)

- ???

5) Need to address the risk created by the interoperability of systems (e.g. merging different sets of data collected for specific purposes)

- Interoperability of systems is only being considered on an aggregated level in terms of organisational architecture and business models -> data protection risks created by the interoperability of systems are not being considered as such

6) Need to address the risk of using location technologies and it's impact to the proportionality principle and privacy

- Data processed within Safespot may qualify as location data (art. 2 (c) Directive 2002/58/EC: data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service). In that case the specific legal provisions in relation tot location data need to be taken into account (Directive 2002/58/EC)

Data protection issues:

7) Safespot vision on privacy by design and BAT?

- Within the Safespot project there are no specific research activities in relation to security and data protection issues in terms of privacy by design and BAT.
- SAFESPOT will follow the leading EC projects (e.g SeVeCom, PRECIOSA)



Thank you for your attention !

k.vanwees@rechten.vu.nl