

Secure Vehicle Communication



SEVECOM (SE-cure VE-hicle COM-munication)

General Introduction





Outline

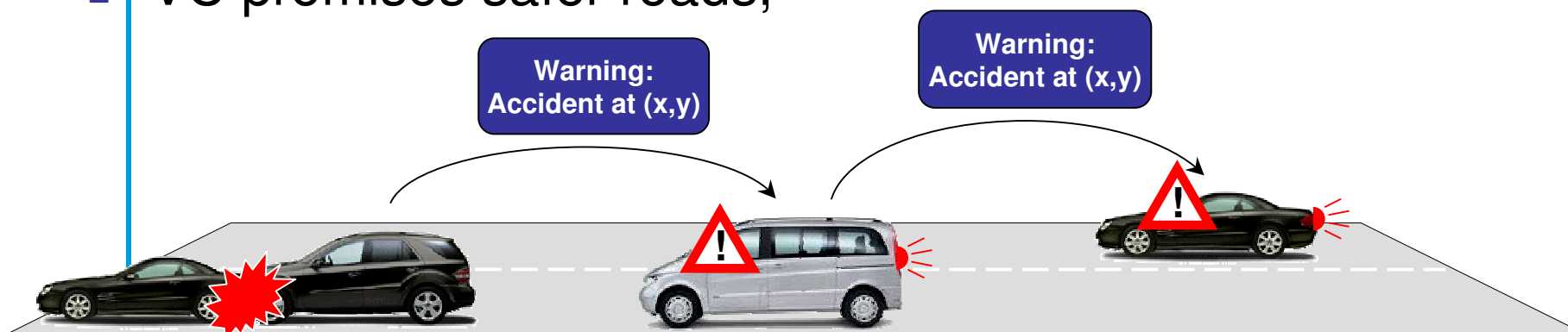
- Vehicle Communication
- Security and Privacy Threats
- Research topics
- Preliminary results



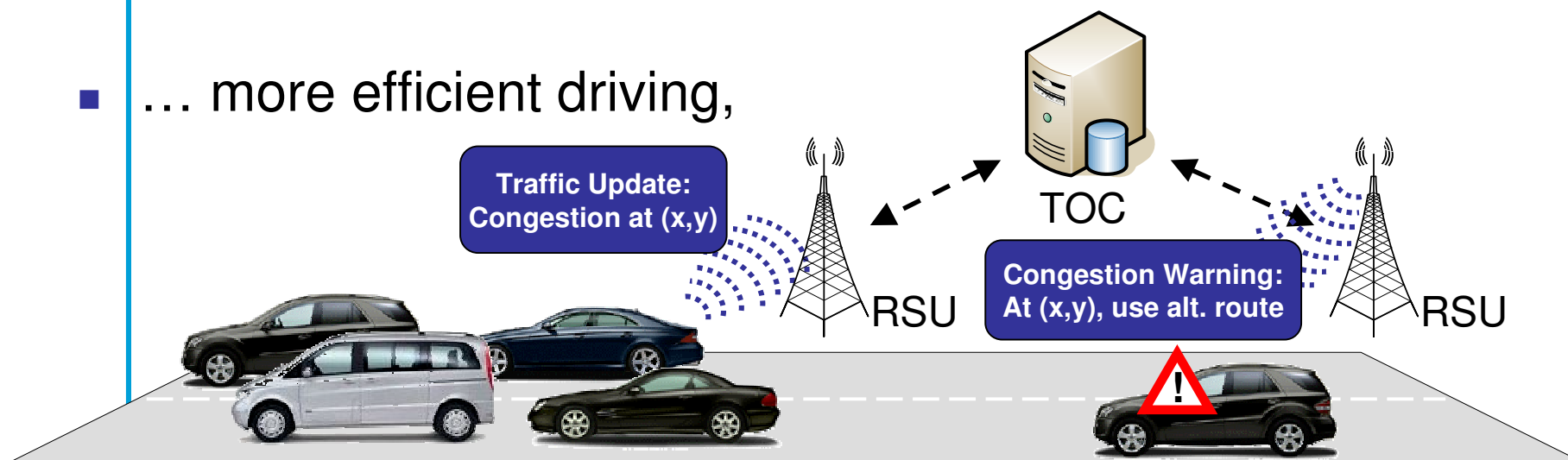
Vehicle Communication (VC)

SEVECOM

- VC promises safer roads,



- ... more efficient driving,

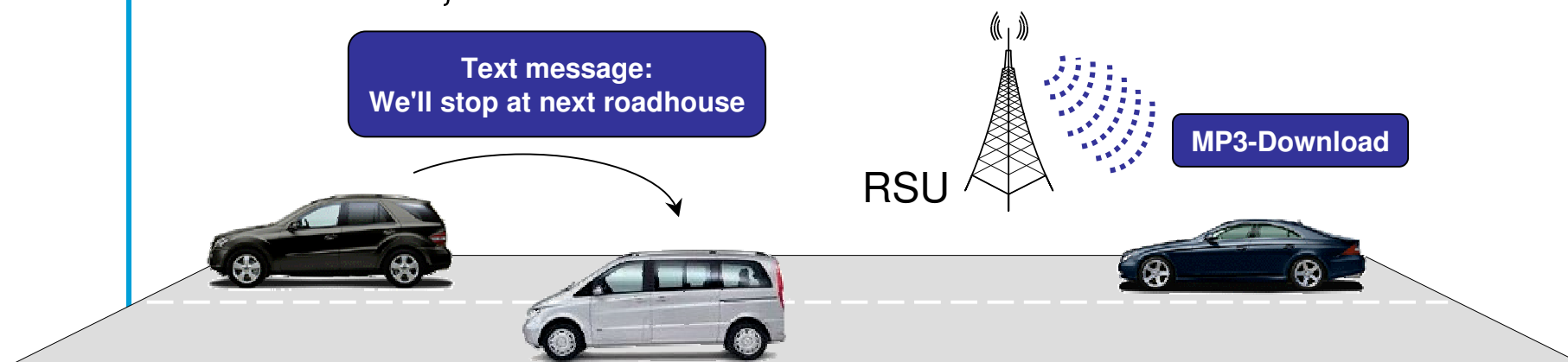




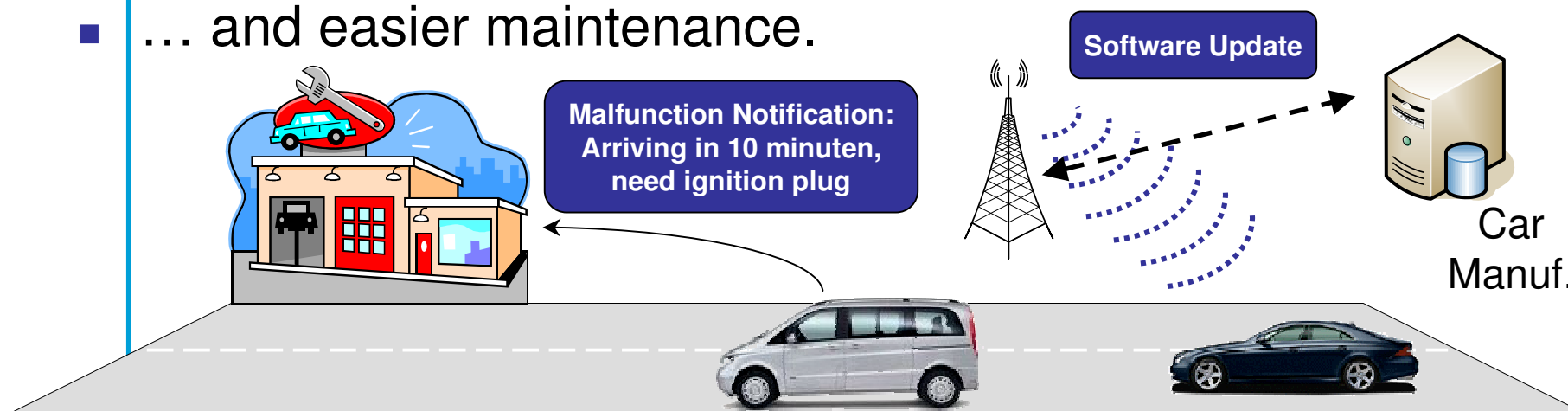
Vehicle Communication (VC)

SEVECOM

- ... more fun,



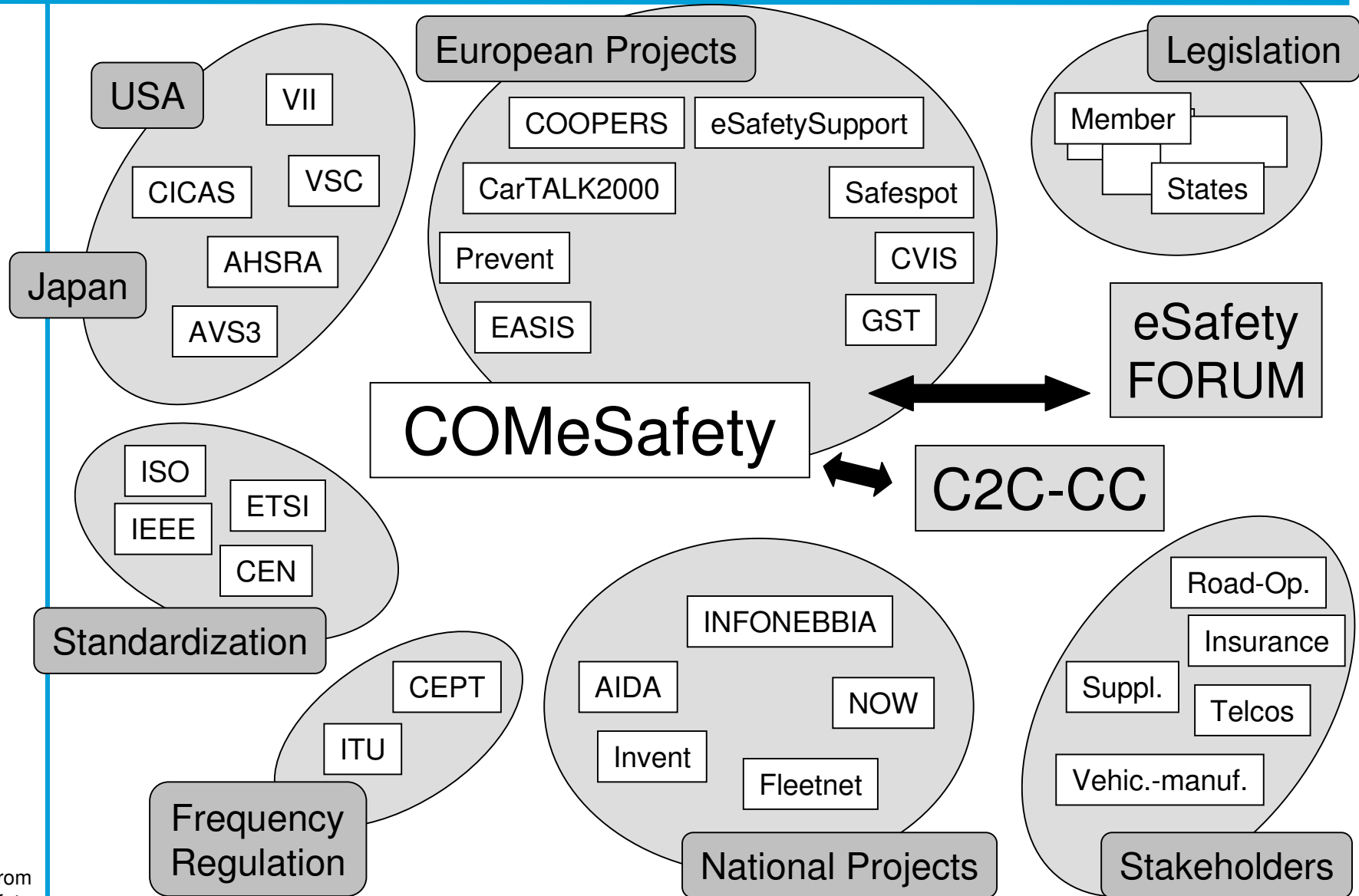
- ... and easier maintenance.





Involved Parties (Europ. Perspective)

SEVECOM

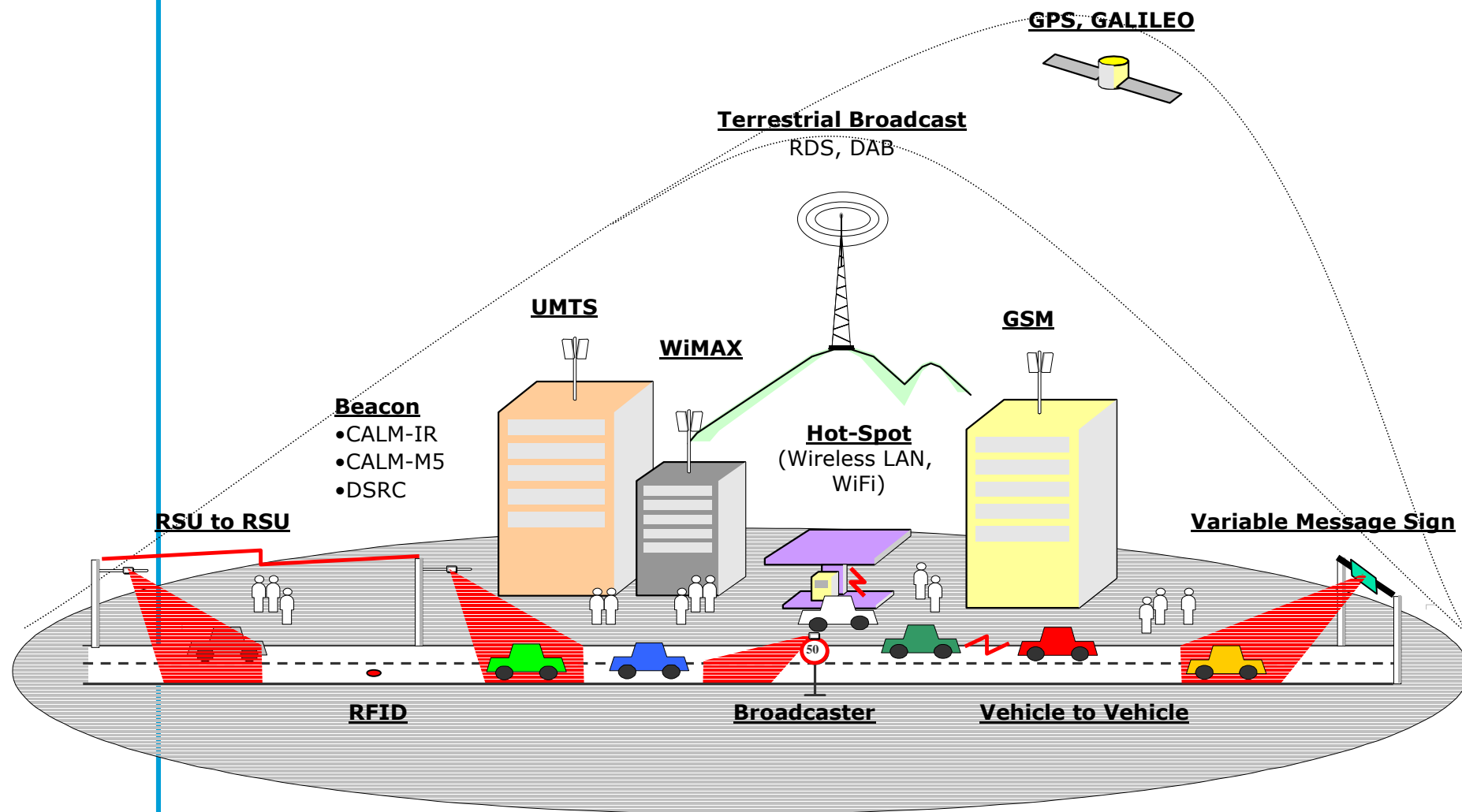


adopted from
COMeSafety



Lot of Involved Technologies

SEVECOM





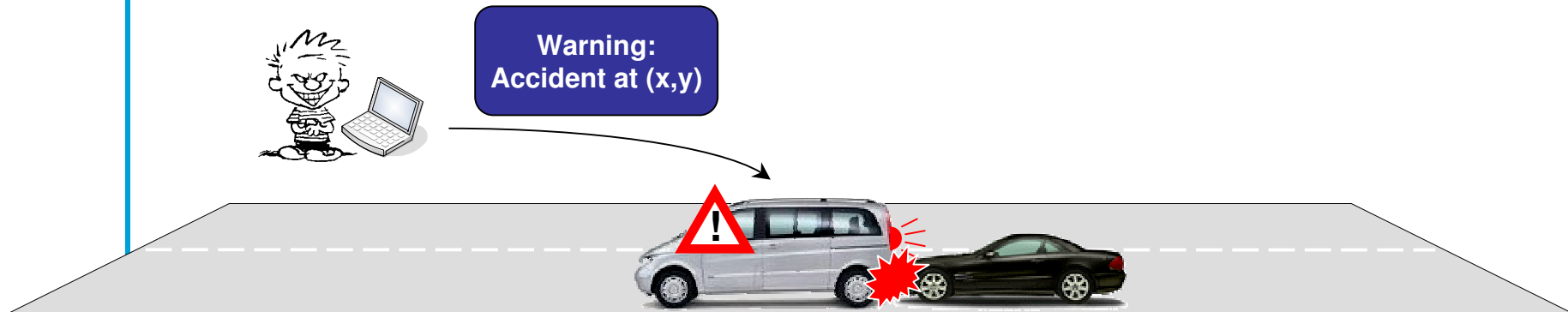
Sounds good



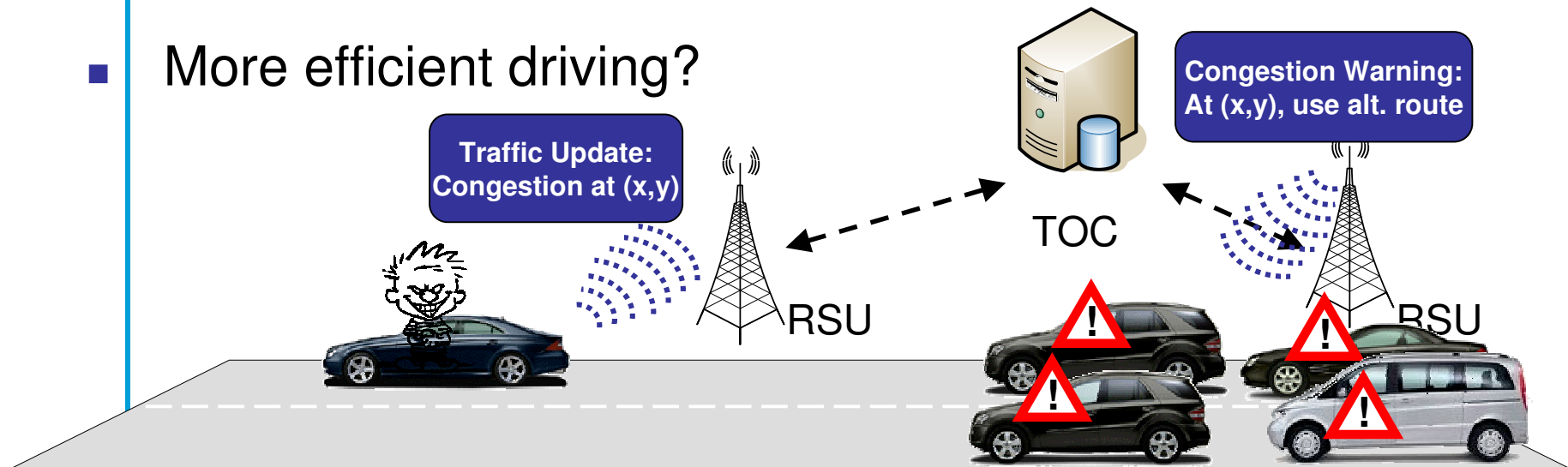


Security and Privacy???

- Safer roads?



- More efficient driving?





Security and Privacy???

SEVECOM

- More fun, but for whom?

Text message from silver car:
You're an idiot!



RSU

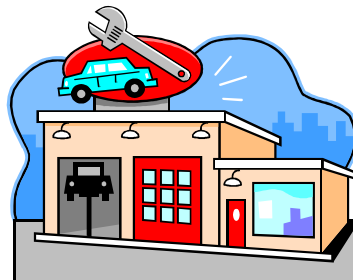
Location Tracking



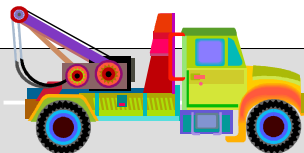
Position Beacon



- ... and a lot more ...



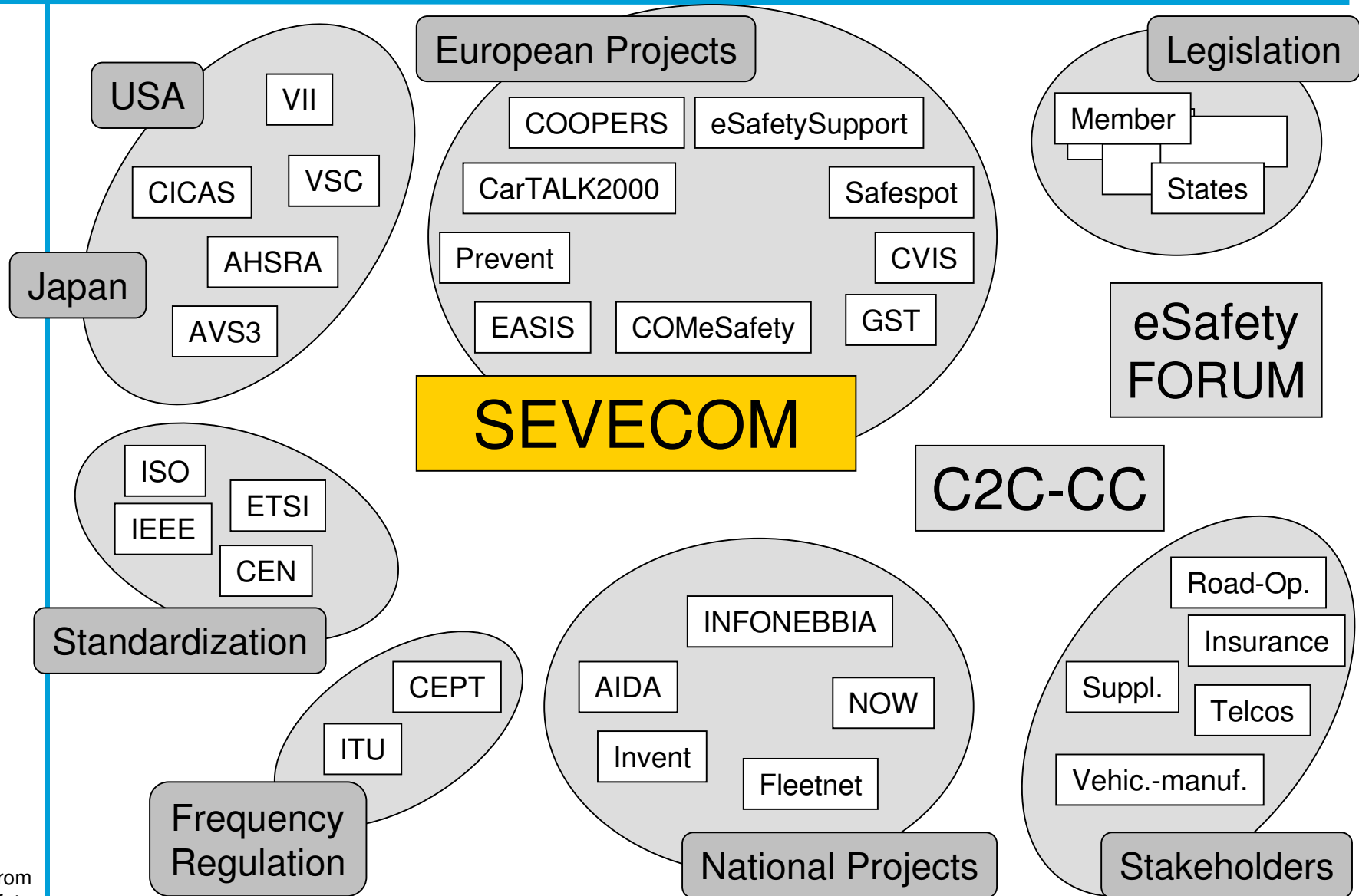
Your new
ignition-control-software





Involved Parties (Slightly modified 😊)

SEVECOM



adopted from
COMeSafety



Objectives

- Large projects have explored and will explore vehicular communications
 - Fleetnet, NOW, CVIS, Safespot, Coopers, ...
 - But no solution can be deployed if not properly secured
- Problems and Opportunities
 - A real setting with real scenarios and applications
 - Very dynamic network with high speeds and real-time constraints
 - Real-world constraints, e.g. who will pay for CA?
 - No energy constraints
 - Contradictory expectations (e.g. position vs. privacy)
- SEVECOM will focus on:
 - Identification of threats against the communication system, transferred data, and the vehicle itself
 - Specification of a usable security architecture
 - The definition of suitable cryptographic primitives



- Mission:
future-proof solution to the problem of V2V/V2I security
- IST STREP Project. 1/1/2006-1/1/2009
- Partners
 - Trialog (Coordinator)
 - DaimlerChrysler
 - Centro Ricerche Fiat
 - Philips
 - Ecole Polytechnique Fédéral de Lausanne
 - University of Ulm
 - Budapest University of Technology and Economics

T/R/I/A/L/O/G

DAIMLERCHRYSLER



PHILIPS





Research topics

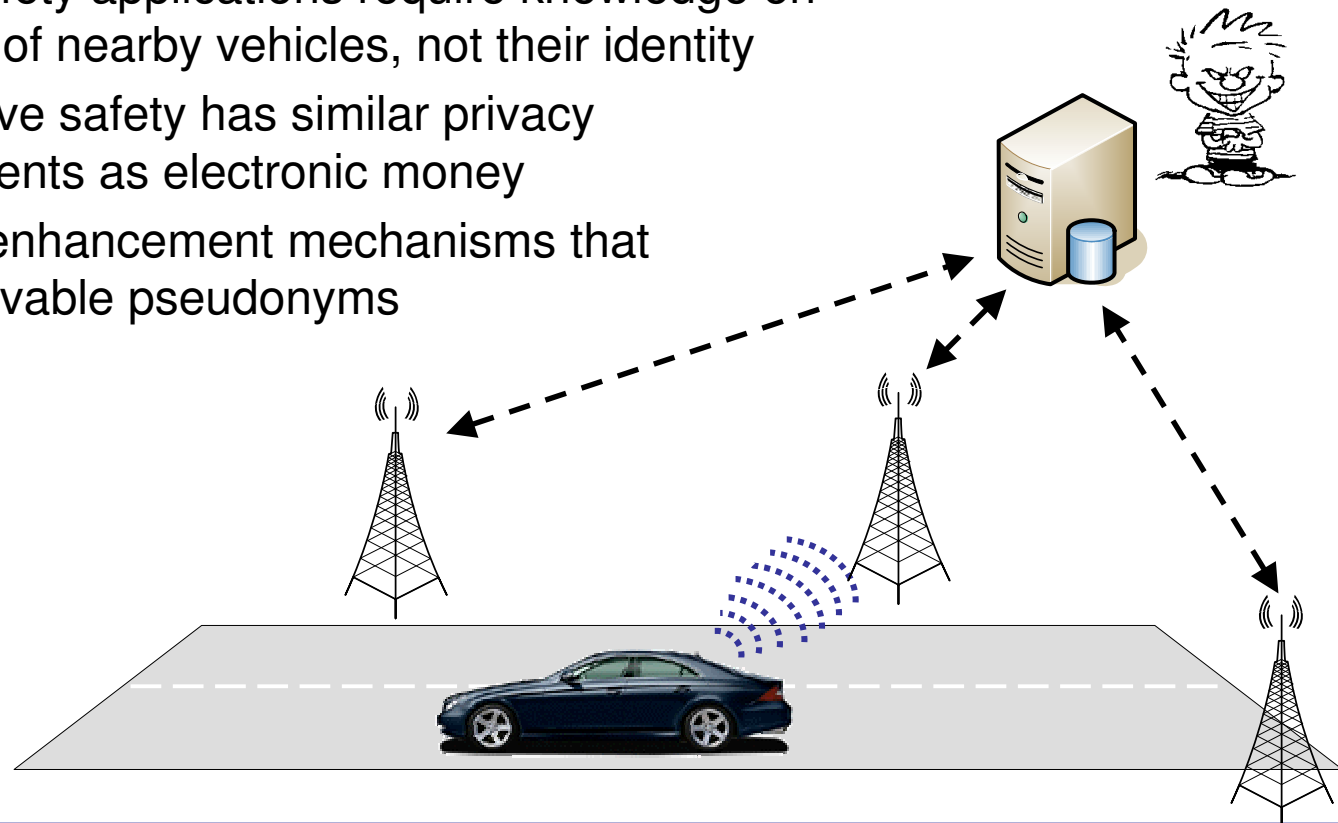


	Topic	Scope of work
A1	Key and identity management	Fully addressed
A2	Secure communication protocols (inc. secure routing)	Fully addressed
A3	Tamper proof device and decision on cryptosystem	Fully addressed
A4	Intrusion Detection	Investigation work
A5	Data consistency	Investigation work
A6	Privacy	Fully addressed
A7	Secure positioning	Investigation work
A8	Secure user interface	Investigation work



Example: A6 – Privacy

- V2V / V2I communication
 - should not make it easier to identify or track vehicles
 - should conform to future privacy directives
 - Lack of privacy control will prevent deployment
 - Active safety applications require knowledge on activities of nearby vehicles, not their identity
 - Automotive safety has similar privacy requirements as electronic money
- ➔ Privacy-enhancement mechanisms that use resolvable pseudonyms





Work Packages

- WP1: Requirements
- WP2: Architecture and Security Mechanisms Specification
- WP3: Focused Development and Integration into Selected Infrastructure
- WP4: Integration in Use Cases
- WP5: Approaches for Security Evaluation
- WP6: Liaison, Dissemination and Exploitation
- WP7: Project Management



Timetable

2006	2007	2008
WP1 Requirements		
	WP2 Architecture/Analysis	
	WP2 Specification	
		WP2 Topics Investigation
	WP3 Development	
		WP4 Use case Integration



- Analyzed properties and security requirements of 56 potential applications
- Selected 10 representative applications using cluster analysis techniques
- Described ~30 different attacks on these applications
- Derived needed security mechanisms to prevent these attacks, e.g.
 - Authentication, location verification, resolvable anonymity, consistency checking, tamper-resistant communication system, ...

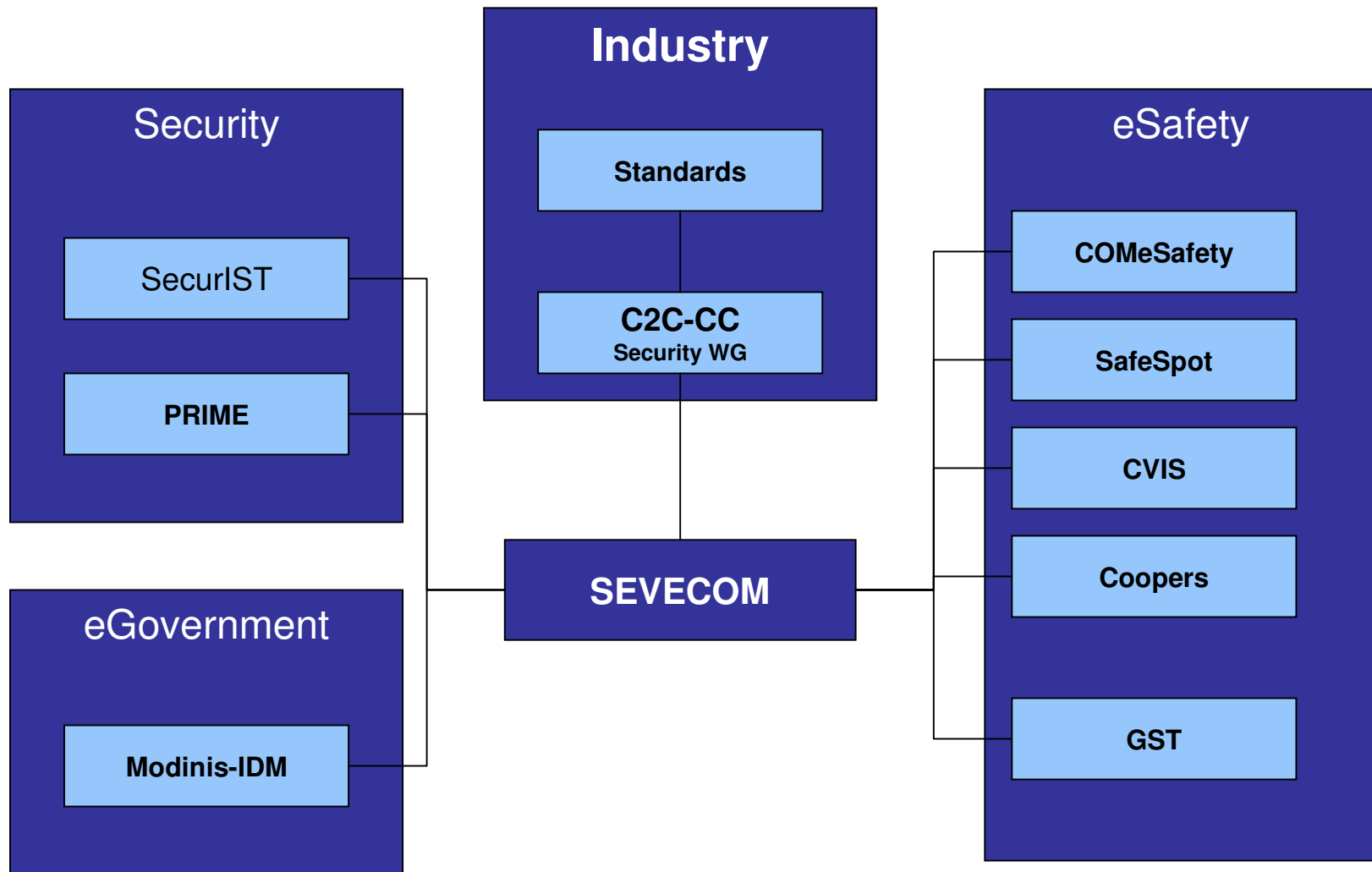


WP2 work started

- Design an architecture that is
 - modular
 - flexible
 - dynamically configurable at runtimeto adapt to the needs of different applications
- Integrate with application solutions by other projects
 - CVIS
 - Safespot
 - Coopers



SEVECOM is a Transversal Project





SEVECOM Contacts



General information	www.sevecom.org	info@sevecom.org
Budapest University of Technology & Economics	Levante Buttyan	+36 1 463 1803 buttyan@crysys.hu
DaimlerChrysler	Rainer Kroh	+49 731 505 2862 rainer.kroh@daimlerchrysler.com
Ecole Polytechnique Fédérale de Lausanne	Jean-Pierre Hubaux	+41 21 693 26 27 jean-pierre.hubaux@epfl.ch
Fiat Research Center (CRF)	Stefano Cosenza	+39 011 90 83076 stefano.cosenza@crf.it
Philips	Hans-Jürgen Reumerman	+49 241 6003 629 hans-j.reumerman@philips.com
TRIALOG	Antonio Kung	+33 144 70 61 03 antonio.kung@trialog.com
Ulm University	Frank Kargl	+49 731 50 31310 frank.kargl@uni-ulm.de