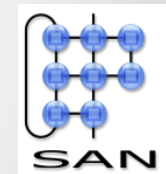


# Car Connections

Johan Lukkien



System Architecture  
and Networking

# Smart mobility, TU/e wide

Cooperative Driving (platooning), A270: Helmond-Eindhoven, 2011  
(Mechanical Engineering/TNO)



Full electric: Lupo (ME)



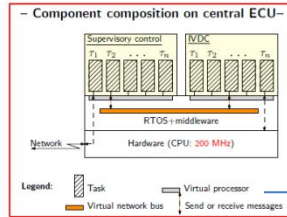
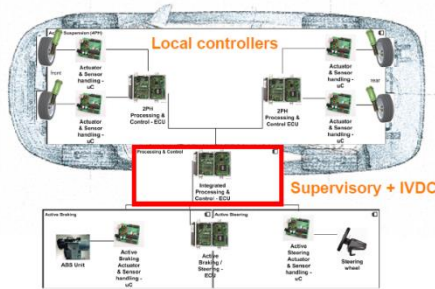
Full Solar: Stella



Strategic Area Smart Mobility

# Smart mobility, TU/e wide

- 4X Local controllers for steering, braking, suspension;
- Front and rear IVDC;
- 1X Global IVDC state estimation and supervisory control.



M&CS, ME

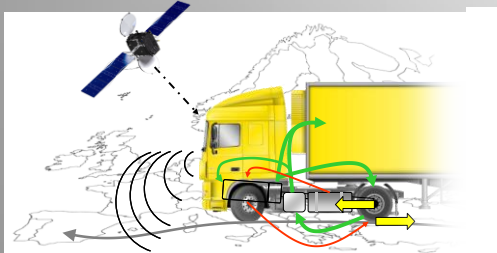
(Semi-)independent developed components by various partners!



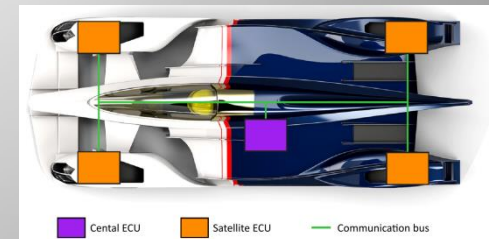
Hybrid Innovations for Trucks (HIT) project

Safety-Critical Domain Certification

InMotion, Solar Team, "Cars in Context" TU/e projects



Functional safety methodology (PDEng projects)



# Agenda

- Privacy, Safety and Security
- Intelligent Transport Systems overview
  - Communication ‘spheres’
    - within the vehicle
    - inter vehicle: short and long range
- Security in short range communication
  - applications, and architecture
    - US and EU schemes
  - safety, privacy
  - current viewpoints
- Security within the vehicle
- Conclusion and outlook

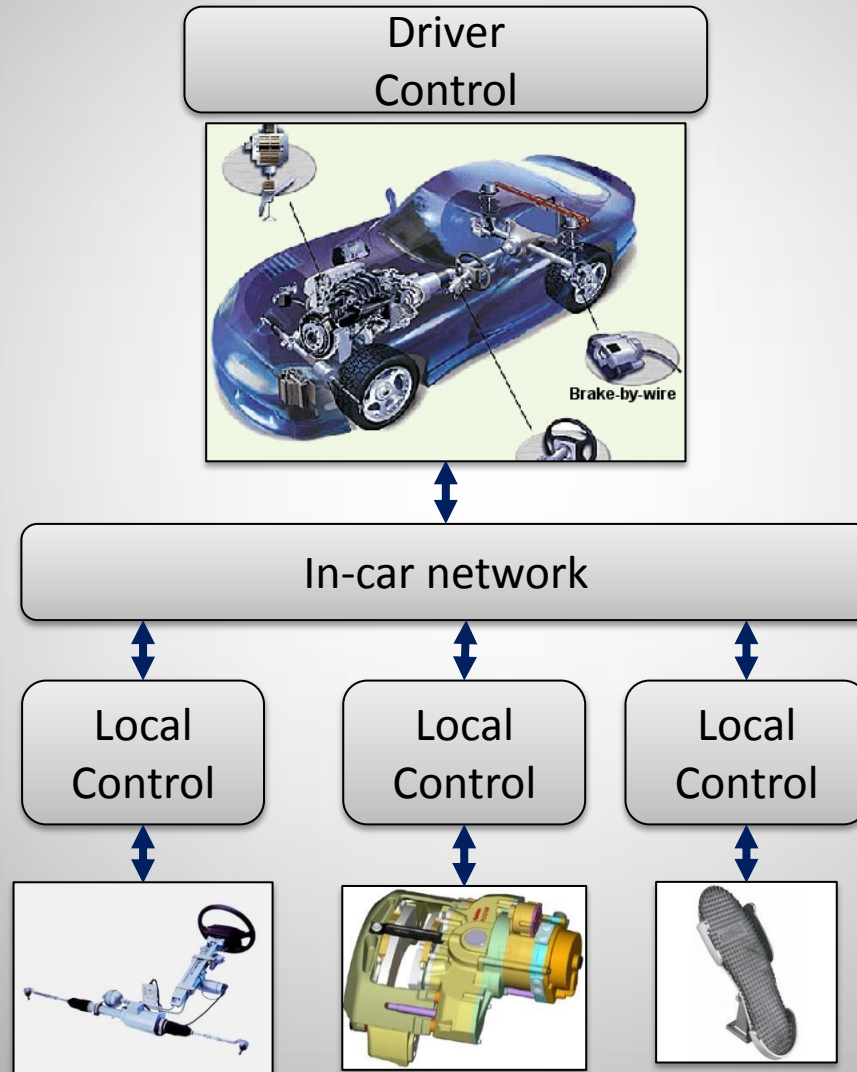
# Privacy, Safety, and Security

- **Privacy:** control over personal information
- **Safety:** freedom from danger or risk on injury resulting from recognized but potentially hazardous events
- **Security:** regulating access to (electronic) assets according to some policy
  - *policy*: allowed and disallowed actions
  - *security mechanisms*: can be regarded as enforcing the policy
- Privacy and safety restrictions result in security policies
  - security for privacy and security for safety

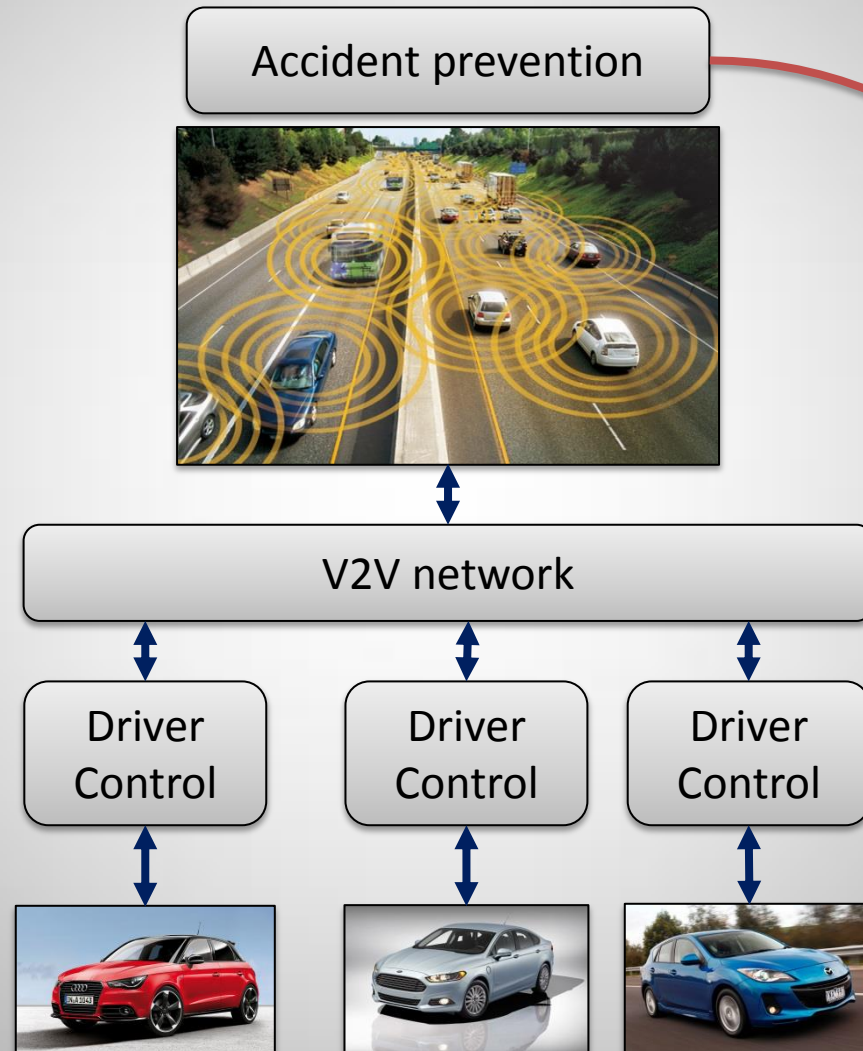
# Requirements

- Examples:
  - Safety:
    - safety violations by malicious external parties must be prevented
    - safety must be maintained while executing regular functions (functional safety)
  - Privacy:
    - personal data must remain under control of the owner
- Leads to *Common Criteria, classification of functions and development process (ISO 26262), certification*
- Sounds rather abstract, so, let's look at some details....

# Vehicles operate using networked ICT



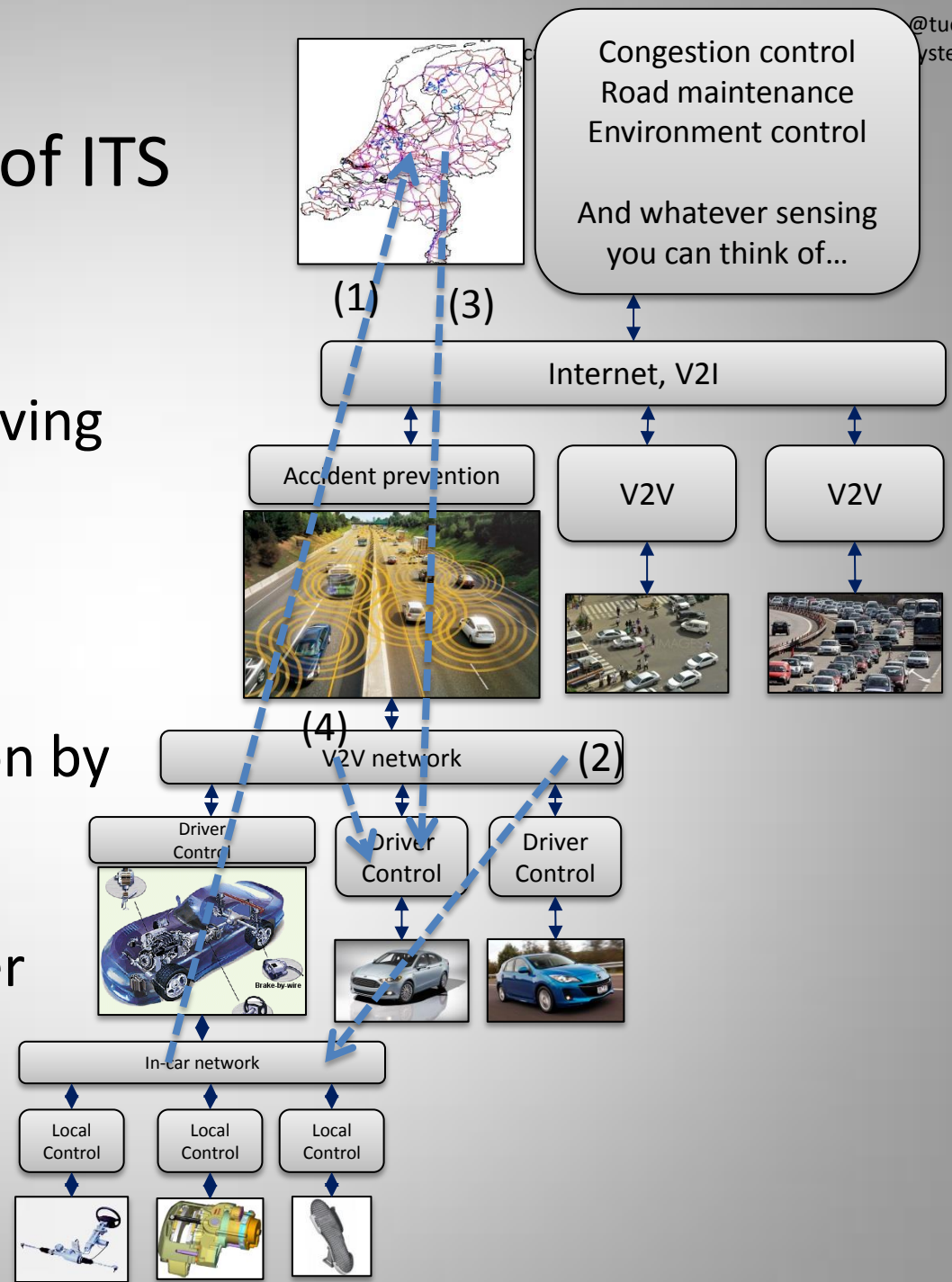
# Vehicles become parts of a larger whole



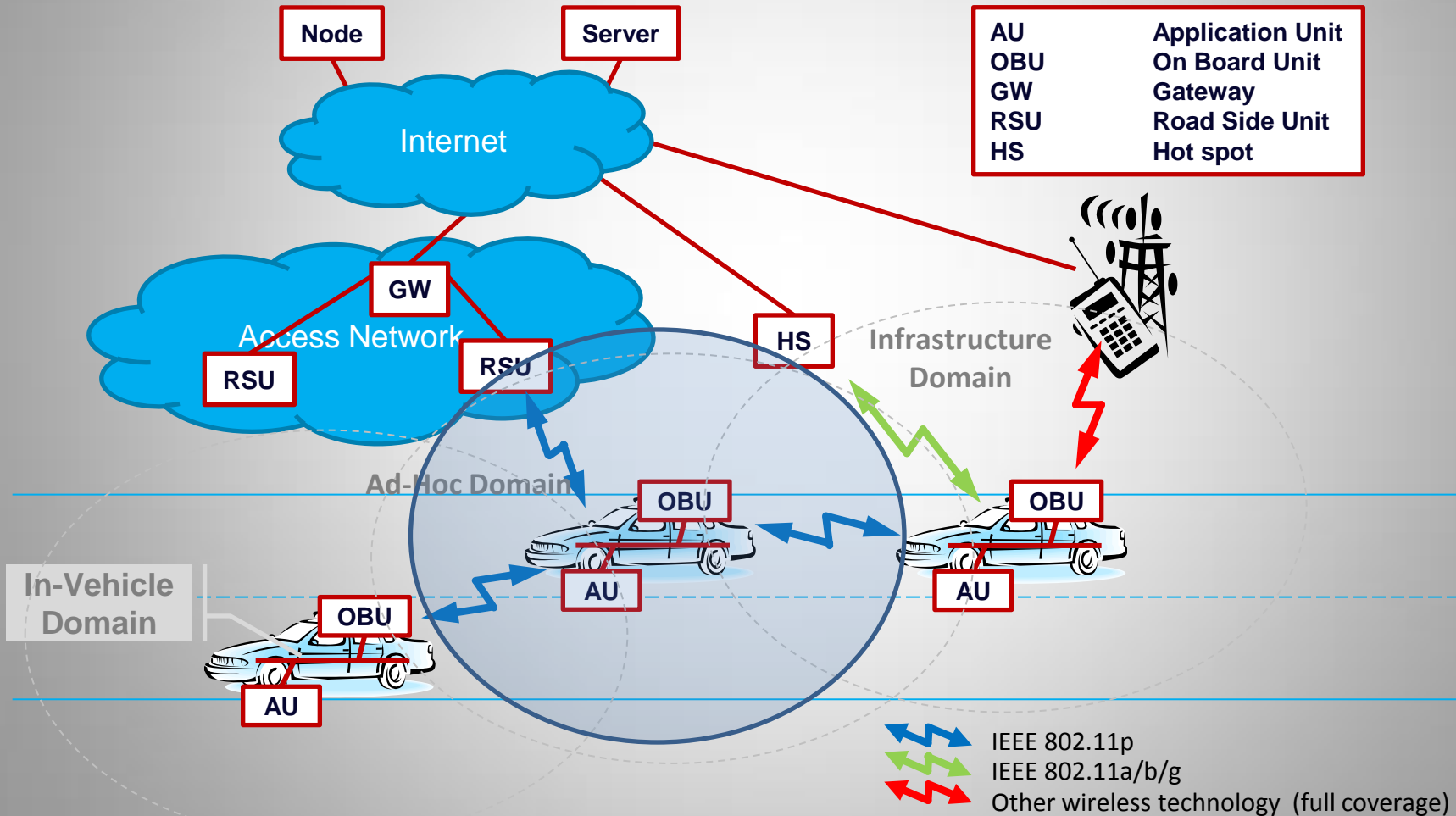


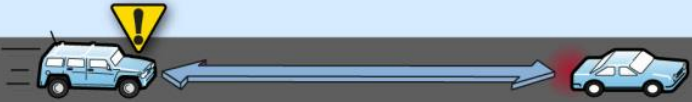




# A conceptual view of ITS

- Example data flows:
  - (1) gather detailed driving data to determine
    - local weather
    - road condition
  - (2) accident prevention by direct intervention
  - (3),(4) informing driver about upcoming road conditions



# A more detailed view on V2V/V2I



Scenario and warning type	Scenario example
<p><b>Rear end collision scenarios</b></p> <p><b>Forward collision warning</b> Approaching a vehicle that is decelerating or stopped.</p>	
<p><b>Emergency electronic brake light warning</b> Approaching a vehicle stopped in roadway but not visible due to obstructions.</p>	
<p><b>Lane change scenarios</b></p> <p><b>Blind spot warning</b> Beginning lane departure that could encroach on the travel lane of another vehicle traveling in the same direction; can detect vehicles not yet in blind spot.</p>	
<p><b>Do not pass warning</b> Encroaching onto the travel lane of another vehicle traveling in opposite direction; can detect moving vehicles not yet in blind spot.</p>	
<p><b>Intersection scenario</b></p> <p><b>Blind intersection warning</b> Encroaching onto the travel lane of another vehicle with whom driver is crossing paths at a blind intersection or an intersection without a traffic signal.</p>	

Source: GAO analysis of Crash Avoidance Metrics Partnership information.

# How does this work?

- It is *cooperative*
- Two different approaches, same network technology (802.11p)
  - **US**: Wireless Access in Vehicular Environments – WAVE, using single-hop broadcast
  - **EU**: ETSI TC ITS standards, using Geo-networking
- Essentially: vehicles emit *periodically* or *event-driven* status information
  - called *Basic Safety Messages* (BSM, US)
  - and *Cooperative Awareness Messages* (CAM, EU)

# Some application examples (BSM ~SAE J2735)

Apps.	Comm.type	Freq.	Latency	Range
Lane Change Warning	V2V, periodic, P2M	10Hz	100ms	150m
Collision Warning	V2V, periodic, P2M	10Hz	100ms	150m
Emergency Brake Lights	V2V, event-driven, P2M	10Hz	100ms	300m
Pre-Crash Sensing	V2V, event-driven, P2P	50Hz	20ms	50m
Stop Sign Assists	I2V and V2I, periodic	10Hz	100ms	250m
Left Turn Assistance	I2V and V2I, periodic, P2M	10Hz	100ms	300m
Traffic Signal Violation	I2V, periodic, P2M	10Hz	100ms	250m
Curve Speed Warning	I2V, periodic, P2M	1Hz	1s	200m

V2V = Vehicle to Vehicle  
 P2M = Point to Multipoint  
 I2V = Infra structure to Vehicle


*Eight high priority vehicle safety applications as chosen by NHTSA and VSCC.*






*NHTSA – US National Highway Traffic Safety Administration*

*VSCC – Vehicle Safety Communication Consortium of CAMP (Crash Avoidance Metrics Partnership)*

# Security to protect safety in BSM

- A vehicle could perform a (physical) action upon receiving certain messages. This response must be on good grounds, and safe.
  - authentication: does this message really come from
    - that particular car?
    - the car left behind me?
  - authorization: what is allowed
    - by this party?
    - by this message?
  - integrity: was this message not tampered with?
- Further concerns regarding safety:
  - are messages really delivered (and not lost or jammed)?
  - functional safety
    - maintain safe and responsive behavior while executing normal functions

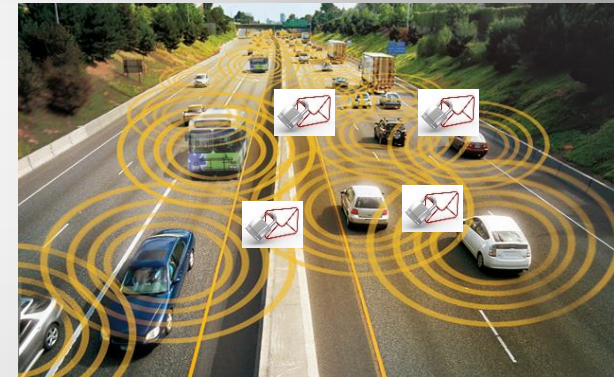


Scenario and warning type	Scenario example
<b>Rear end collision scenarios</b> <b>Forward collision warning</b> Approaching a vehicle that is decelerating or stopped.	
<b>Emergency electronic brake light warning</b> Approaching a vehicle stopped in roadway but not visible due to obstructions.	
<b>Lane change scenarios</b> <b>Blind spot warning</b> Beginning lane departure that could encroach on the travel lane of another vehicle traveling in the same direction; can detect vehicles not yet in blind spot. <b>Do not pass warning</b> Encroaching onto the travel lane of another vehicle traveling in opposite direction; can detect moving vehicles not yet in blind spot.	 
<b>Intersection scenario</b> <b>Blind intersection warning</b> Encroaching onto the travel lane of another vehicle with whom driver is crossing paths at a blind intersection or an intersection without a traffic signal.	

Source: GAG analysis of Crash Avoidance Metrics Partnership information.

# *Security to protect privacy in BSM*

- Communication might reveal sensitive information
  - location of vehicle, one could track it
  - driver identity, number of passengers
  - driving behavior
- Security mechanisms might add to this
  - e.g. the *signing* of messages
- Hence:
  - policies on data handling, certification of those policies
    - e.g. collect only anonymous data, forbid vehicle tracking in mandatory services
  - requirements on security mechanisms



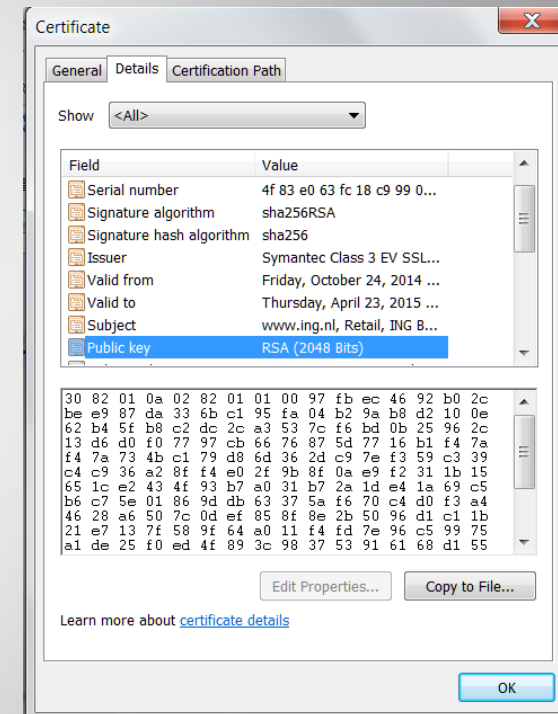
# Requirements on security

- Interoperable
- Process-able in real-time and limited in size (bandwidth)
- Identity-free
- Non-repudiation (sender cannot deny having sent a message)
- Scalable
  - local: few hundreds of vehicles
  - global: millions of vehicles
- Extensible, towards other applications of V2x communication



# Proposal (US)

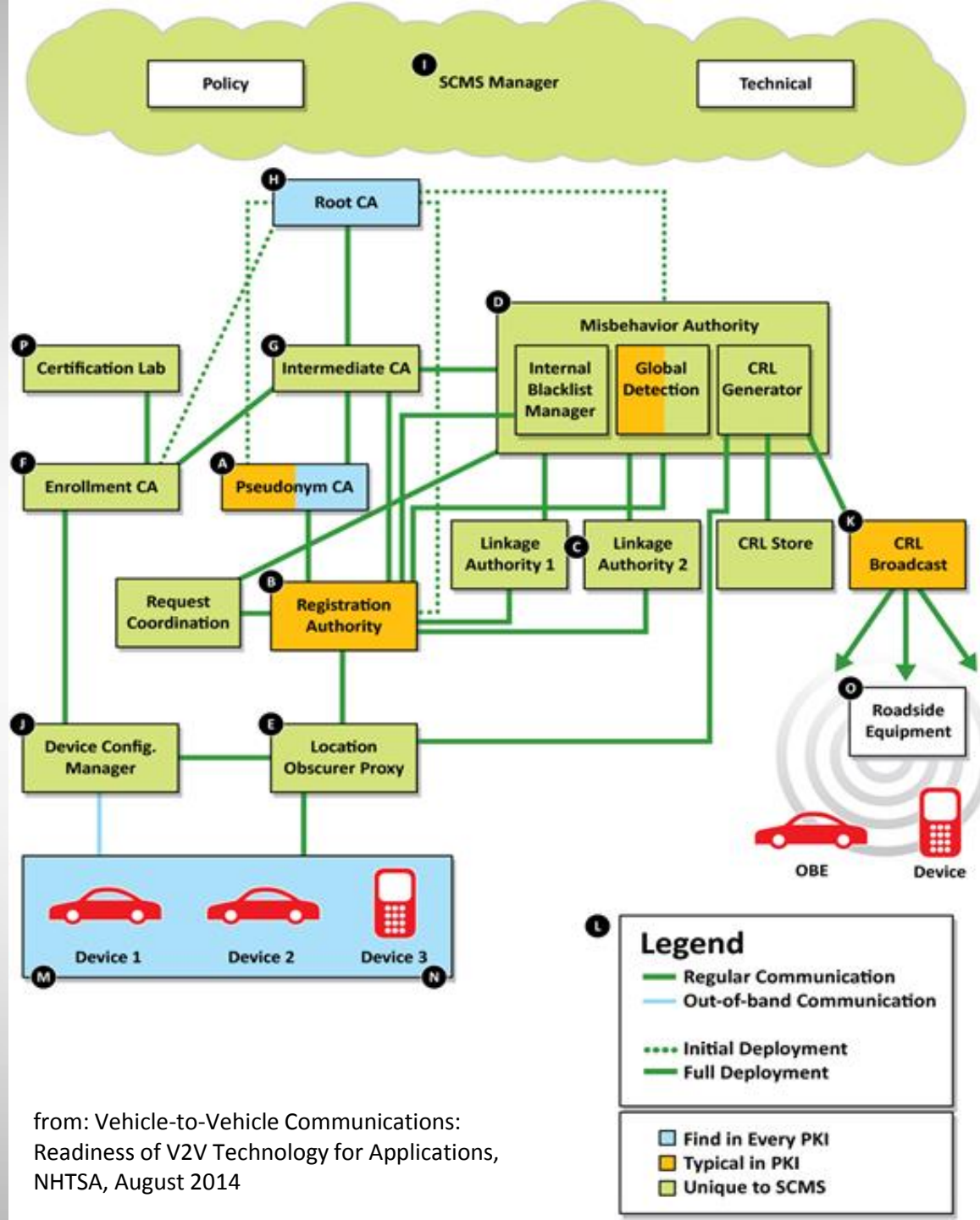
- Use *Public Key Infrastructure* to *sign* messages
  - authentication, integrity & non-repudiation
- *Certificate* associates public and private key
  - decryption using the public key demonstrates:
    - knowledge by the sender of the private key, which is associated with an identity
    - that the message was not altered
- Complex extentions to deal with the specific concerns of these applications
  - intermittent connectivity, anonimity
  - small size certificates, keys and certificates: ECQVI / ECDSA
    - though these require 10 times more processing power



Certificate for ing.nl

# System outline

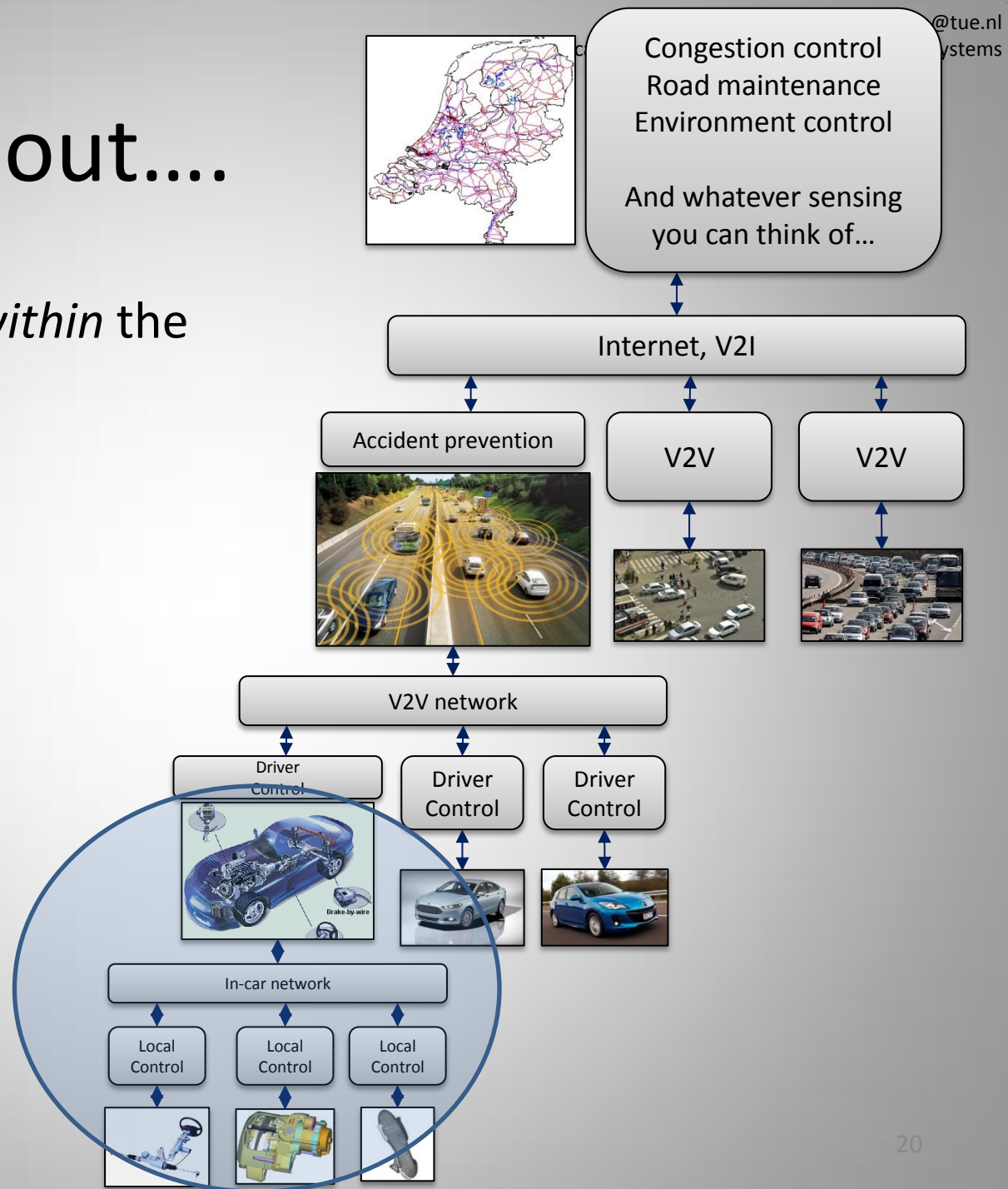
- Comparison: basic PKI / V2x design



from: Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Applications, NHTSA, August 2014

# Zooming out....

- Security concerns *within* the vehicle....

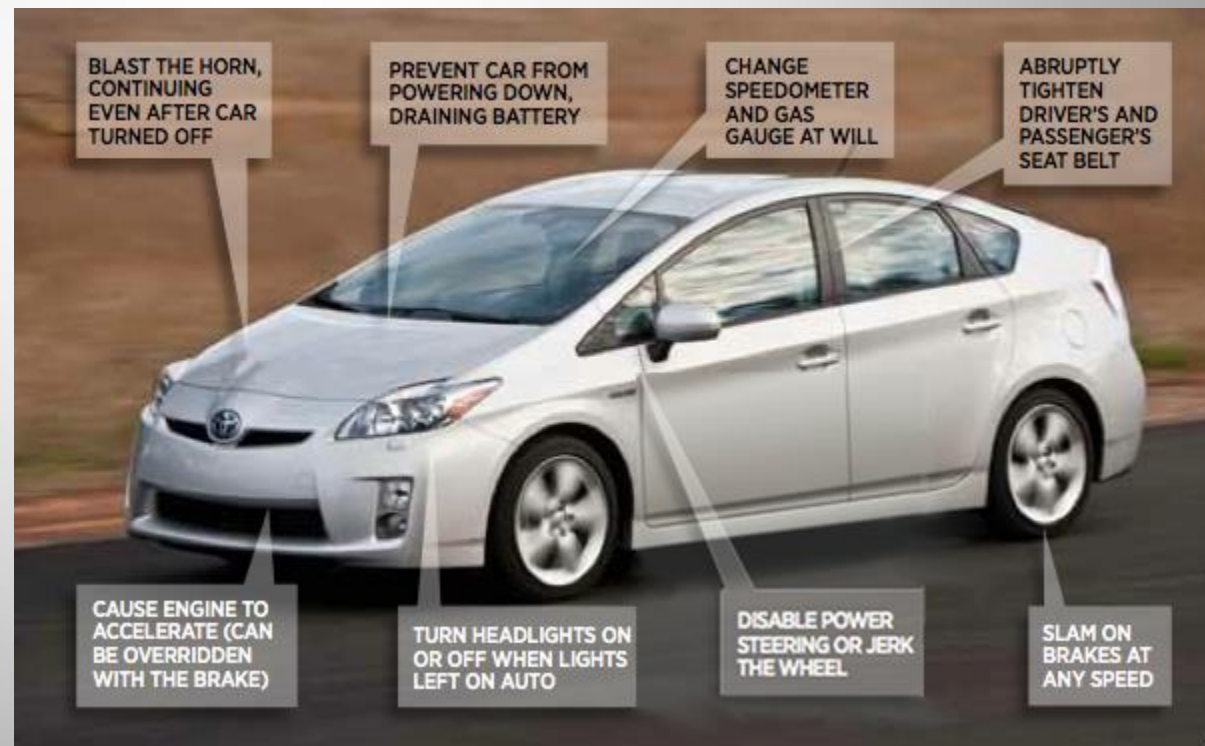


# Hacker with access to internal systems

## Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video)

*This story appears in the August 12, 2013 issue of Forbes.*

- Funny....
- ... but more harmful hacks are possible as well
  - e.g. disabling the brakes
- However, any malicious physical access is dangerous



# Next Generation Vehicle OS



# Concluding remarks

- Security in ITS serves privacy and safety
- Security within the vehicle is lagging behind
- Security between vehicles is being designed in
  
- ITS is a required step towards fully automated driving

# Literature

- Used in this presentation:
  - Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Applications, NHTSA, August 2014
  - Rate-Adaptation Based Congestion Control for Vehicle Safety Communications, PhD thesis Tessa Tielert