

# Car Connections

## Dangerous Liaisons?

Johan Lukkien



# Smart mobility, TU/e wide

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



Full electric: Lupo (ME)



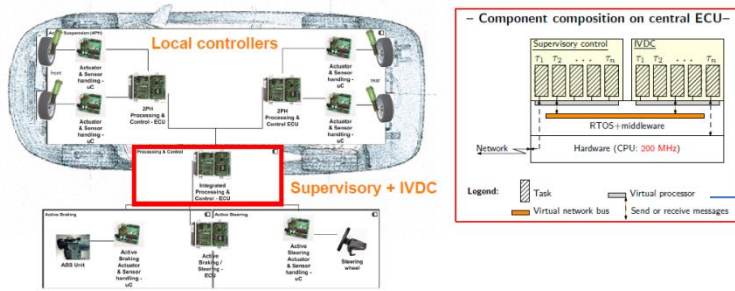
Full Solar: Stella



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.



(Semi-)independent developed components by various partners!



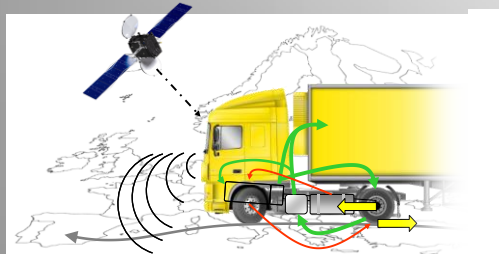
M&CS, ME



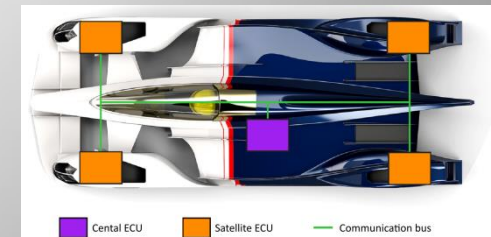
Hybrid Innovations for Trucks (HIT) project

Safety-Critical Domain Certification

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



Functional safety methodology (PDEng projects)



# Agenda

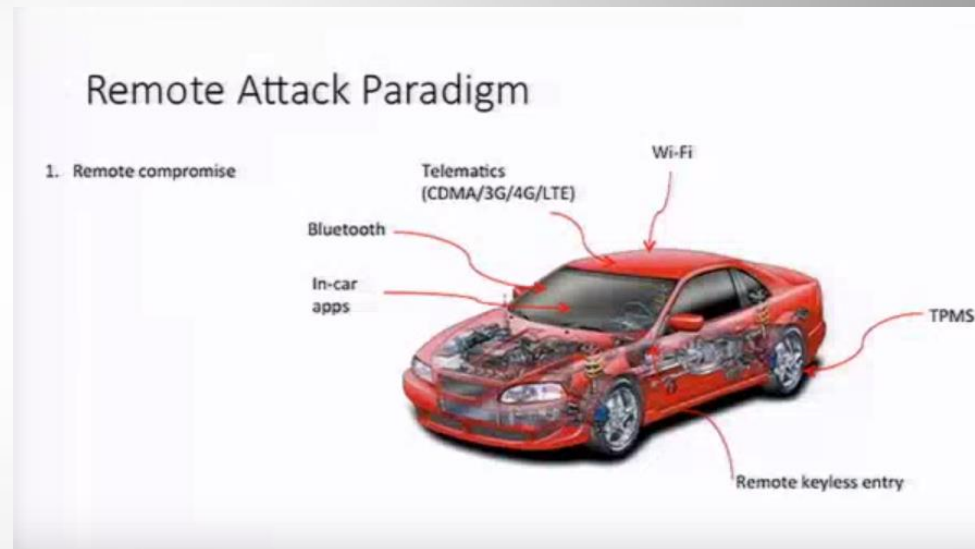
- Privacy, Safety and Security
- Intelligent Transport Systems overview
  - Communication ‘spheres’
    - within the vehicle
    - inter vehicle: short and long range
- Security in short range communication
  - applications, and architecture
    - US and EU schemes
  - safety, privacy
  - current viewpoints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

# Video

<https://www.youtube.com/watch?v=3jstaBeXgAs>

# What changed the game?

- *Internet connectivity*: you can reach a vehicle without leaving your chair
  - as opposed to reaching targeted vehicles physically
- *Wireless connectivity*: of many kinds and types
- *Networks in vehicles*: rather open
- *Automation*: computer does the work of breaking codes
- *Tooling*: advanced hacking tooling readily available as ‘condensed knowledge’
- *Sharing, similarity*: one break-in is enough for all similar vehicles



<https://www.youtube.com/watch?v=OobLb1Mcxnl>

# Privacy, Safety, and Security

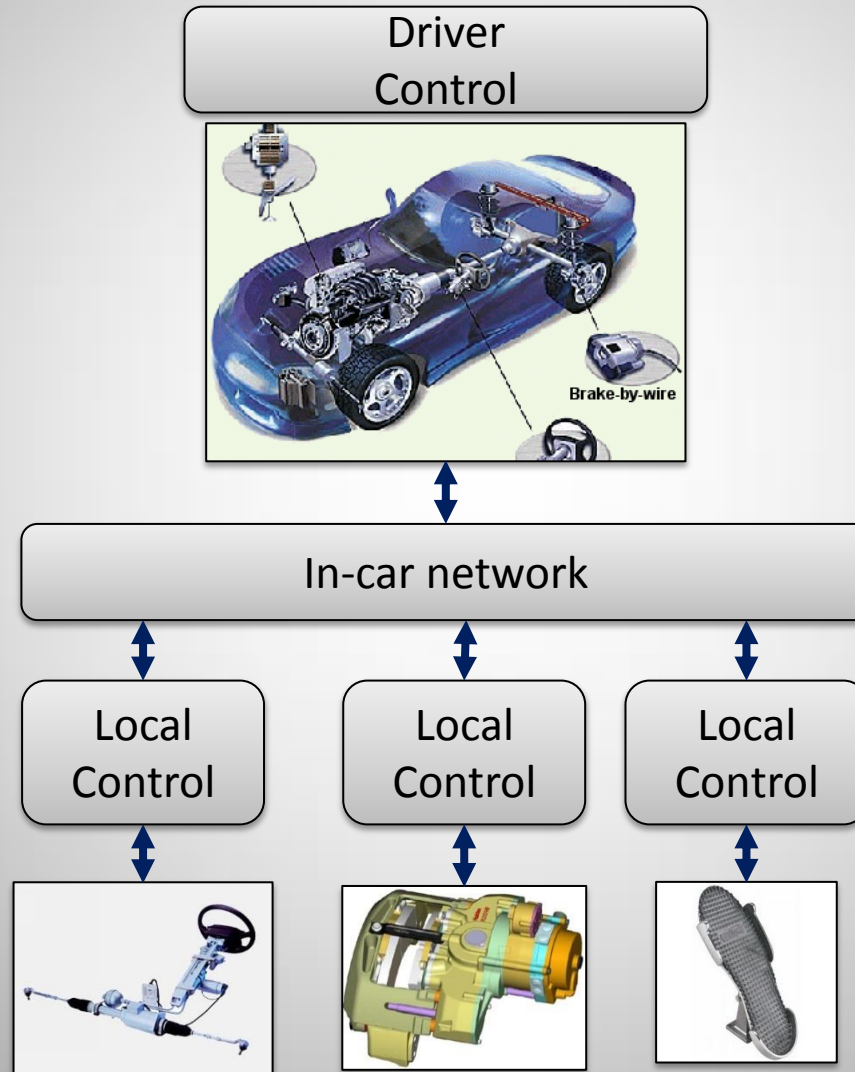
- **Privacy:** control over personal information
- **Safety:** freedom from danger or risk on injury resulting from recognized but potentially hazardous events
- **Security:** regulating access to (electronic) assets according to some policy
  - *policy*: allowed and disallowed actions
  - *security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

# Example requirements

- Safety:
  - safety violations by malicious external parties must be prevented (by a policy of forbidding certain actions)
  - 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....

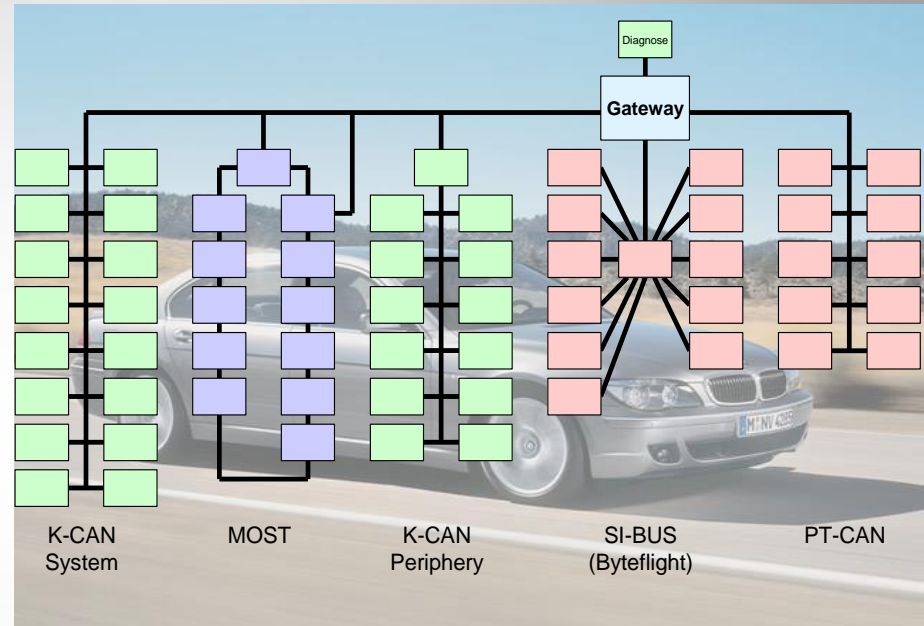


# Vehicles operate using networked ICT



# In-vehicle networks

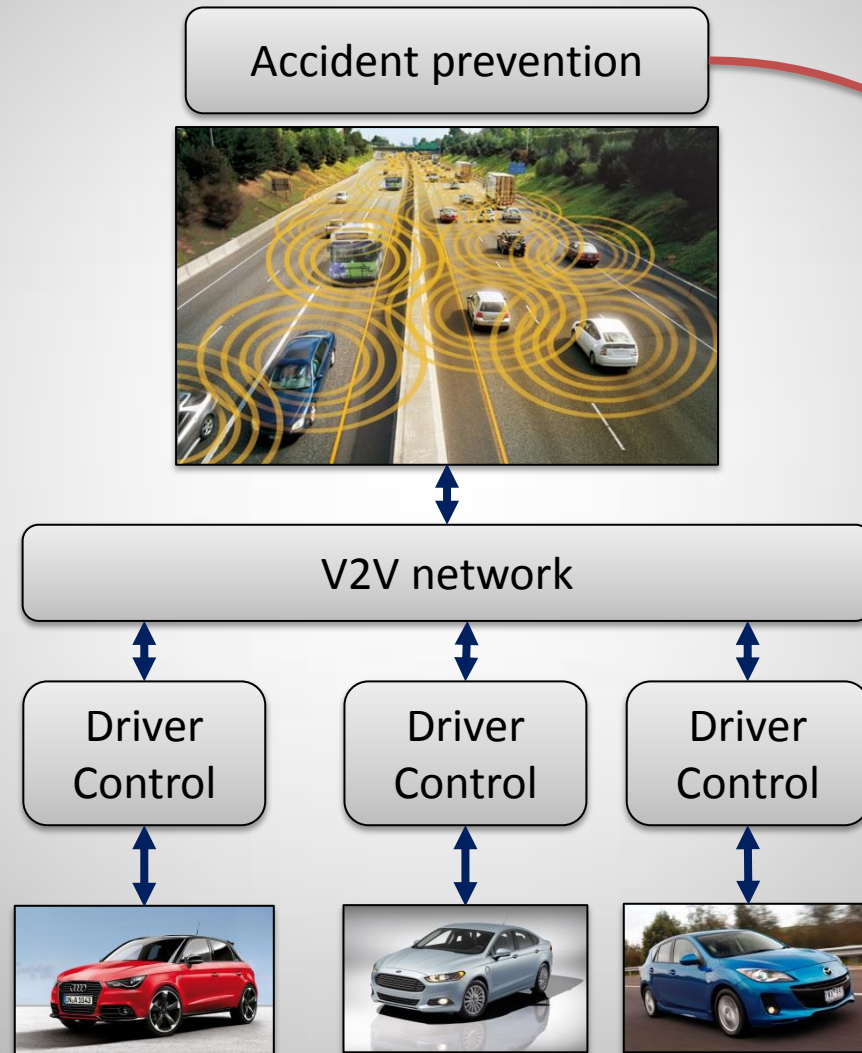
- *Networks of ECUs*
  - 40-80 in a modern car
- Designed for
  - cooperative behavior
  - specialist (remote) management / diagnostics
- Gateway support for *isolation*



BMW 7 series infrastructure

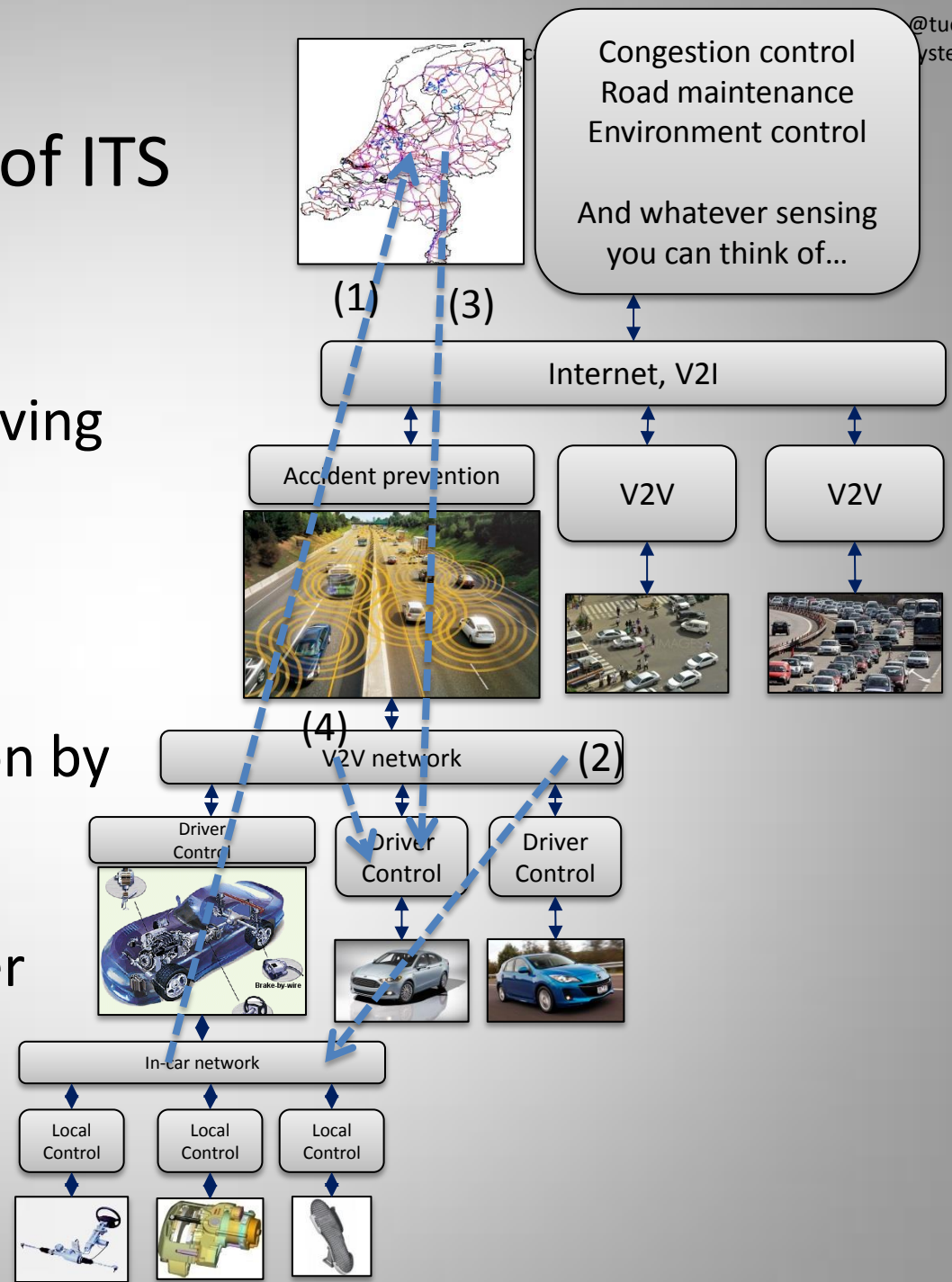
	<b>Flexibility</b>	<b>Predictability</b>	<b>Dependability</b>	<b>Bandwidth</b>	<b>Confidentiality</b>
<b>Powertrain</b>	low	high	high	high	N/A
<b>Chassis</b>	some	high	high	high	N/A
<b>Body/Comfort</b>	some	some	some	low	N/A
<b>Telematics</b>	high	some	low	high	high
<b>Passive Safety</b>	low	high	high	high	N/A

# Vehicles become parts of a larger whole

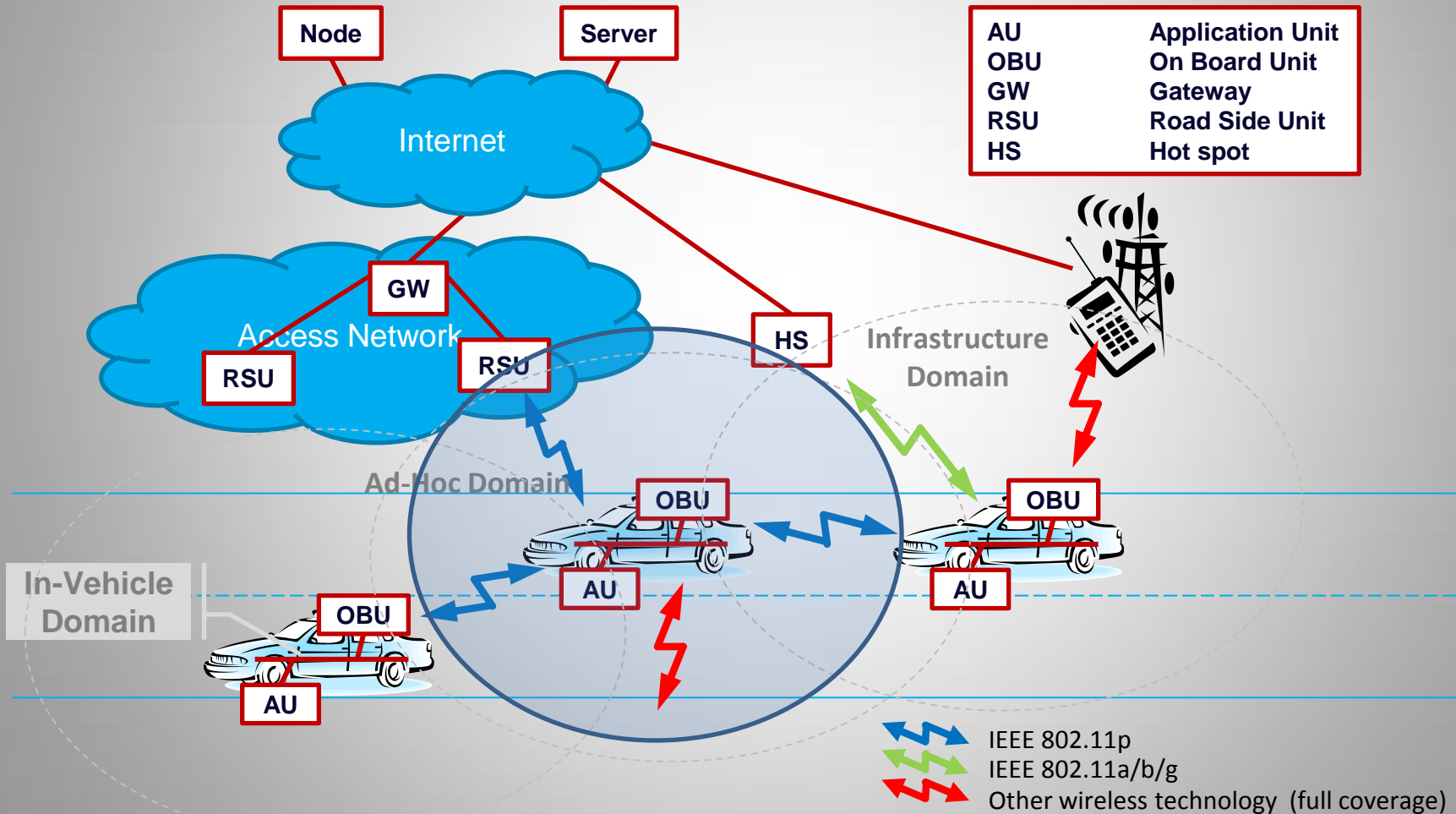


# A conceptual view of ITS

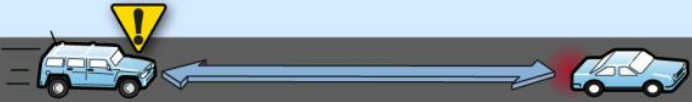




- Example data flows:
  - (1) gather detailed driving data to determine
    - local weather
    - road condition
  - (2) accident prevention by direct intervention
  - (3),(4) informing driver about upcoming road conditions



# 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, dynamic* and *ad-hoc*
- Two different approaches, same network technology (IEEE 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

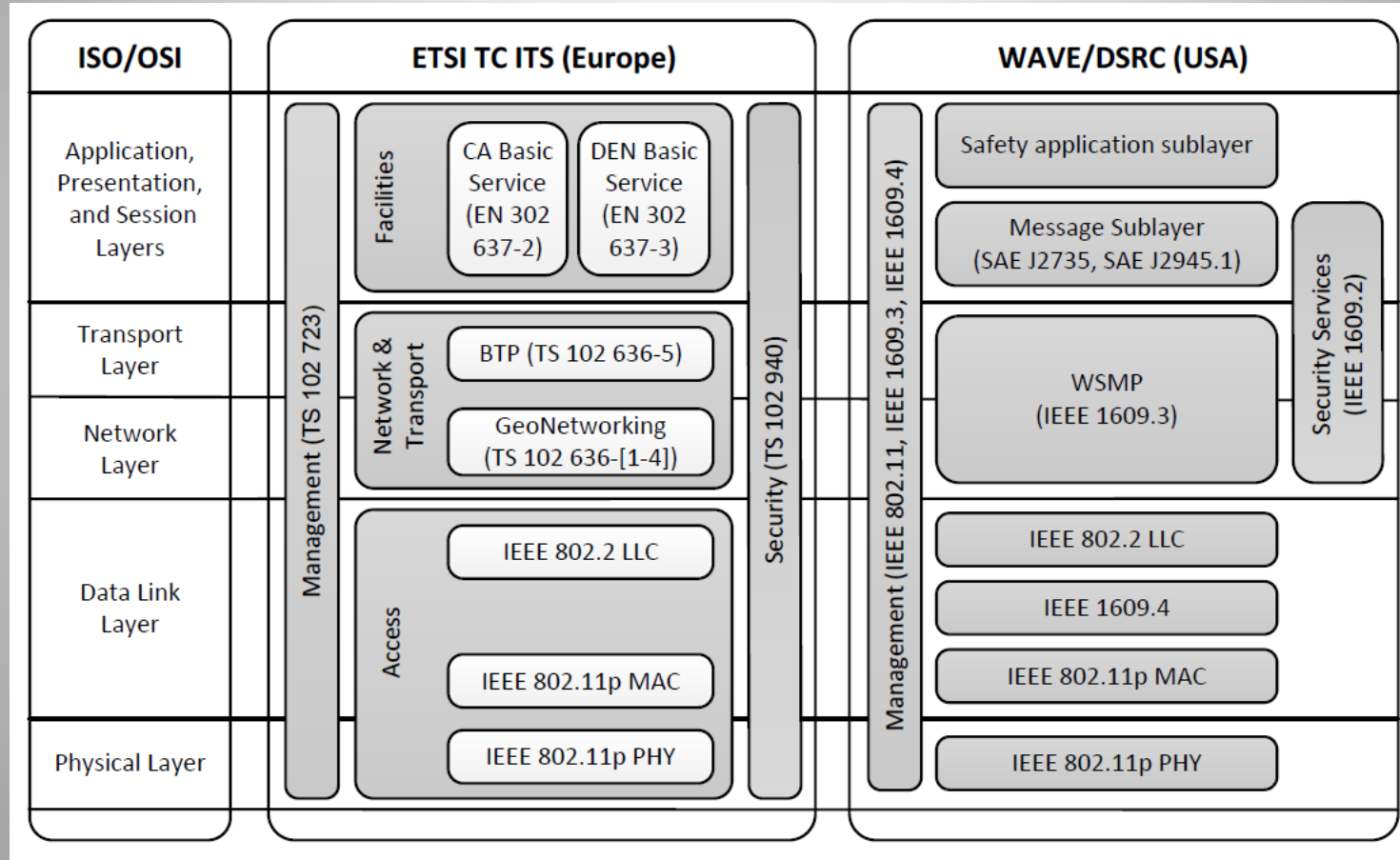
*Eight high priority vehicle safety applications as chosen by NHTSA and VSCC.*

*NHTSA – US National Highway Traffic Safety Administration*

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









# (partial) Communication Stack: EU and US



# 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

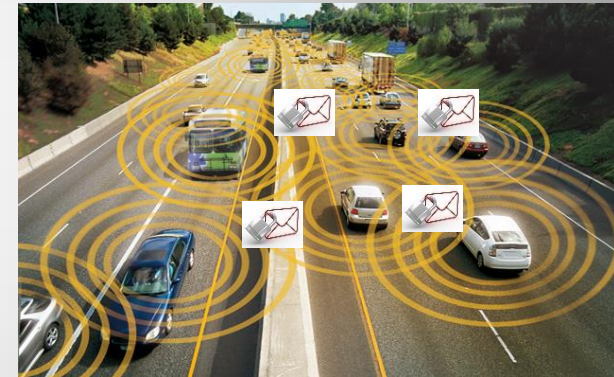


Scenario and warning type	Scenario example
<b>Rear end collision scenarios</b> <b>Forward collision warning</b> Approaching a vehicle that is decelerating or stopped.	
<b>Emergency electronic brake light warning</b> Approaching a vehicle stopped in roadway but not visible due to obstructions.	
<b>Lane 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 reveals the signature
- Hence:
  - policies for data handling, certification of those policies
    - e.g. collect only anonymous data, forbid vehicle tracking in mandatory services
  - requirements on security mechanisms

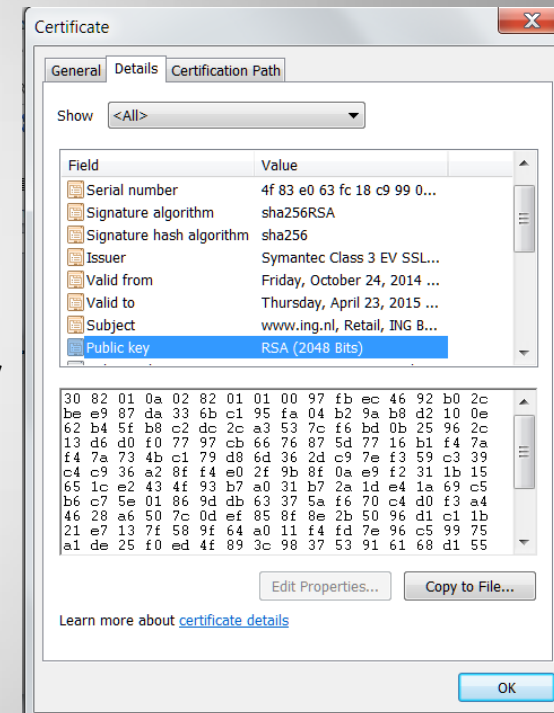


# Requirements on security

- 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)

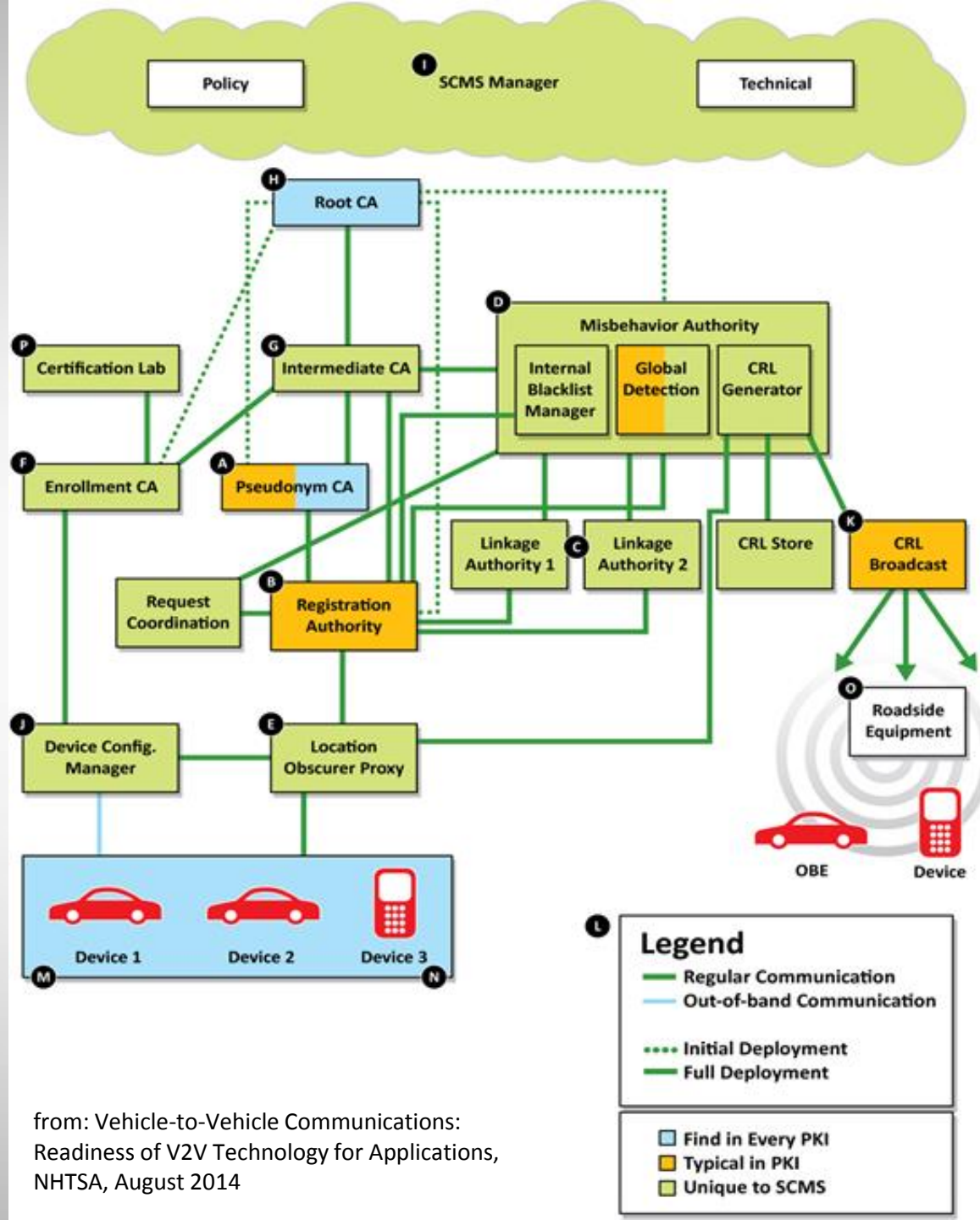
- Use *Public Key Infrastructure* to sign messages
  - authentication, integrity & non-repudiation
- *Certificate* associates public and private key
  - decryption using the public key demonstrates:
    - that the sender knows the private key, which is associated with an identity by an authority
   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



Certificate for ing.nl

# System outline

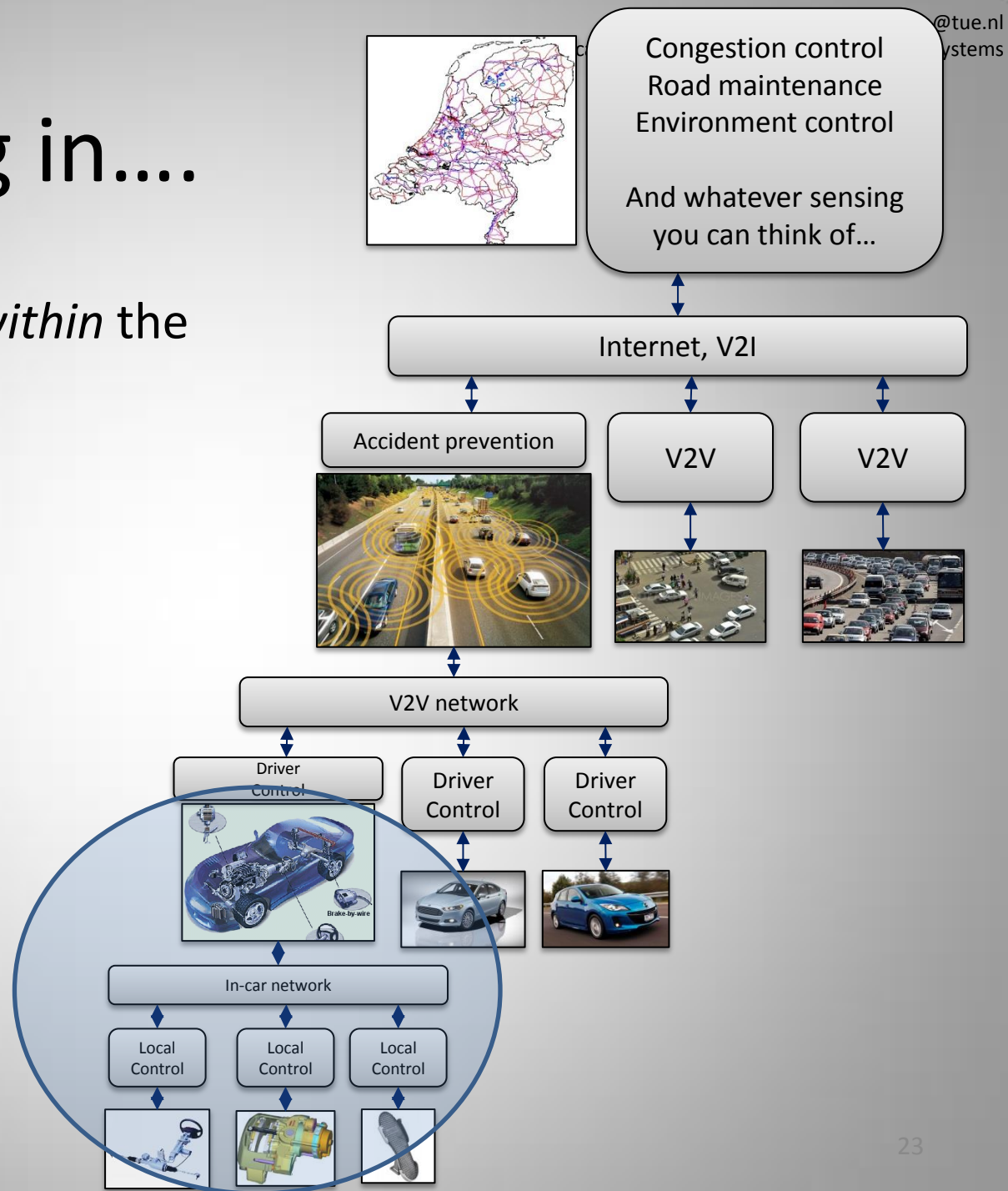
- Security Credentials Management System
- Comparison: basic PKI / V2x design



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

# Zooming in....

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



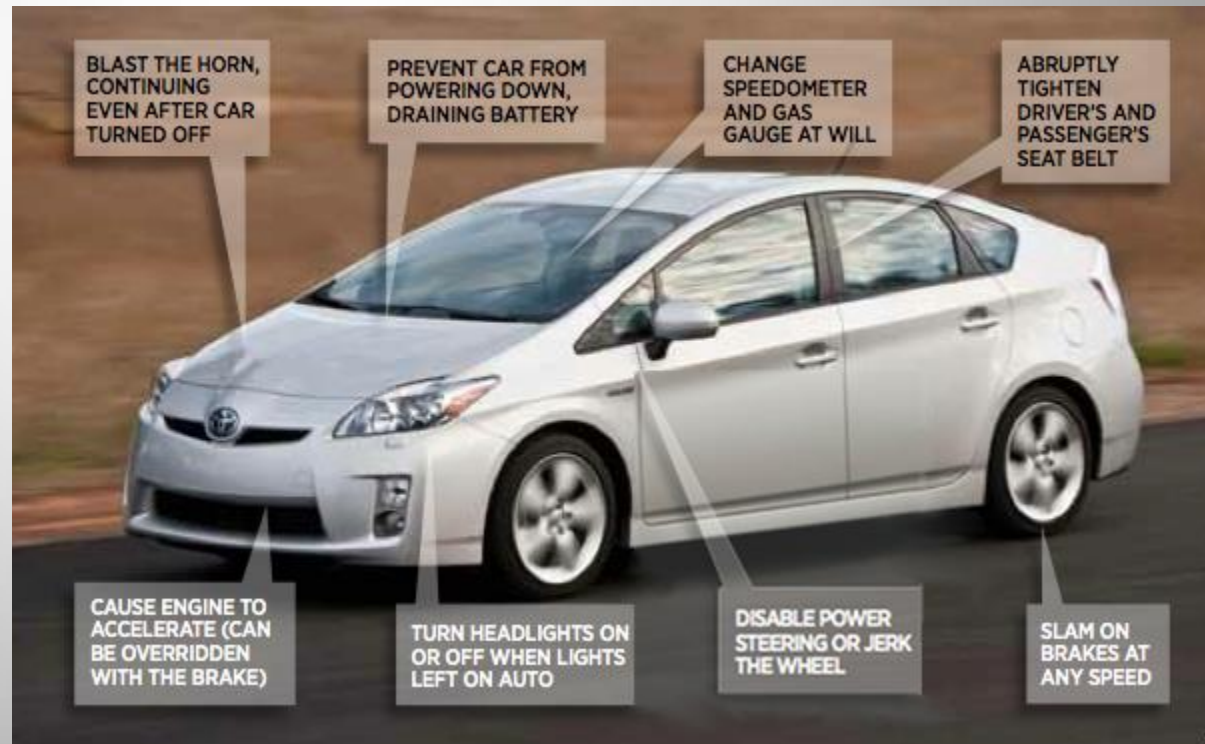


# Hacker with access to internal systems

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

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

- Connecting notebook to CAN bus
- Funny or dangerous, but any harmful hack is possible ...
  - e.g. disabling the brakes
- ... since *any* malicious physical access is dangerous





# When CAN access meets Internet...

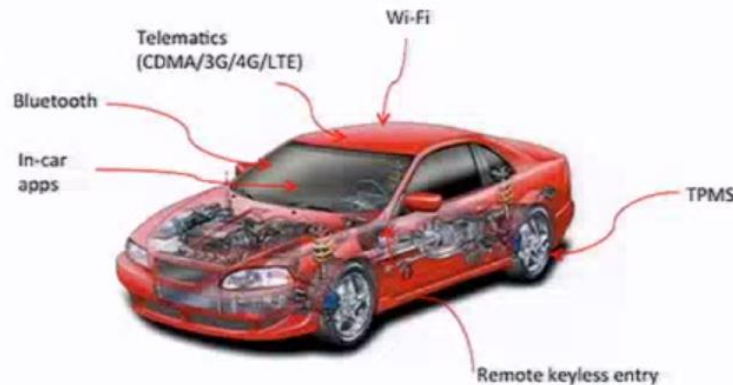
<https://www.youtube.com/watch?v=MK0SrxBC1xs>

# Increasing wireless connections ... and vulnerabilities

- hacking *without* altering the electronics

## Remote Attack Paradigm

### 1. Remote compromise



<https://www.youtube.com/watch?v=OobLb1Mcxnl>

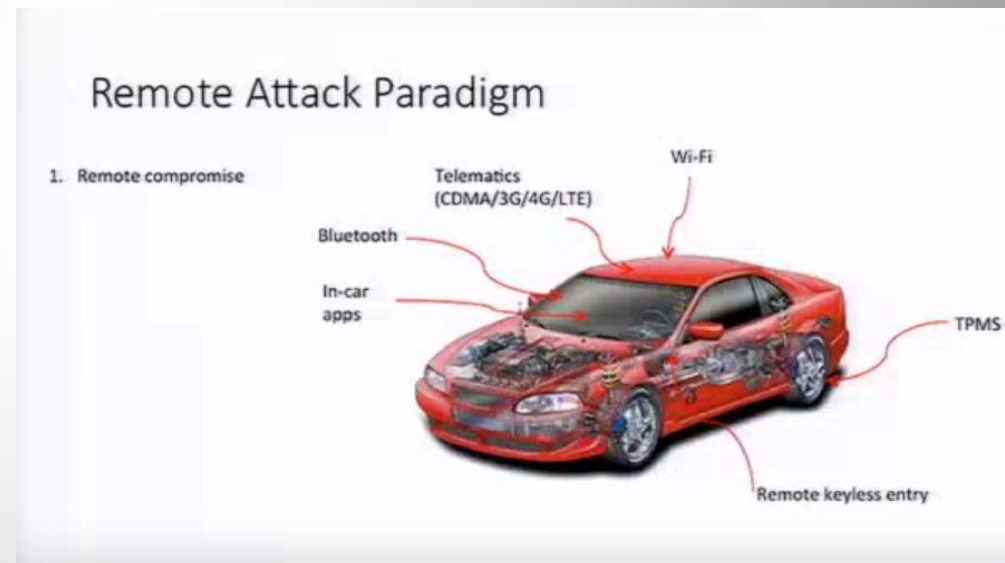
# The drill...

- Attach a module to the CAN bus in order to send and receive control messages and connect to a wireless transceiver

OR

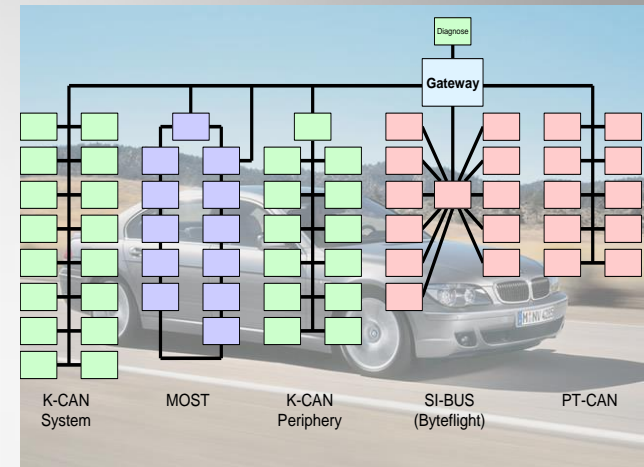
hack into the car via the Internet with the same effect

- Reverse engineer the messaging of this type of car
- Control the car via remote access



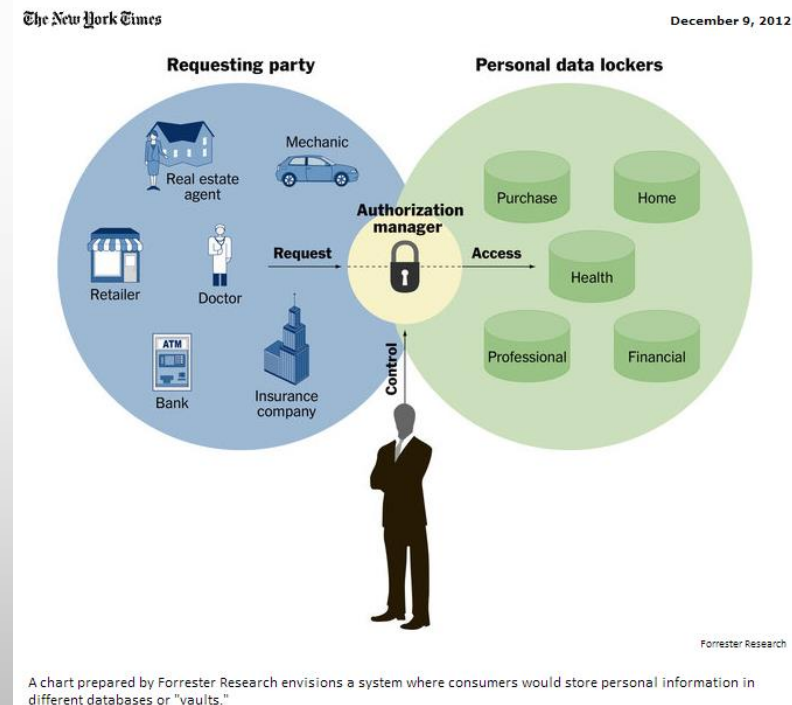
# What to do about this?

- *Protect CAN bus*
  - access control for new CAN devices
  - CAN message signing and encryption
  - ... but who has the keys?
- *Physical separation* – make harmful influence from new components physically impossible
- *Policy separation*
  - implement policies that restrict behavior in certain modes
    - no remote access while driving
    - software update only under specific circumstances, e.g., in a car shop
    - (expose certain behavior while being examined)
- *Self monitoring* – intrusion detection



# What about privacy?

- Policies about what to collect, communicate, store, e.g.,
  - collect only anonymous data
  - forbid vehicle tracking in mandatory services (e.g. road side)... plus certification of these, access tracing, auditing
- A radically different approach to managing data
  - a *personal data store* where data about a person is stored under his control
    - no storage in private repositories of companies



# Next Generation Vehicle OS...



# Adjust design methods

- Attack model becomes more complex:
  - obtaining a virus during a repair
  - downloadable apps
  - all mentioned solutions introduce new vulnerabilities
- This has to become part of the systematic consideration of the safety of all (ICT) functions
  - ISO 26262

# ISO 26262: functional safety

- Safety under performing normal functions
  - avoid excessive risk of normal functions
  - examine – and deal with – common failures [fault → error → failure]
- Explicit ‘safety life cycle’ for automotive products
- ‘Safety goals’ classified in risk classes, are determined for each ‘hazardous event’
  - risk class: ASIL, Automotive Safety Integrity Class
    - QM, ASIL A-D, order of magnitude of risk
    - combination of severity, exposure, controllability
      - e.g S3, E4, C3: life threatening, highly probable, difficult to control (ASIL D)
- Adherence to ISO 26262 expected to increase



# Concluding remarks

- Security in ITS serves privacy and safety
- Security between vehicles is being designed in
- Security within the vehicle is lagging behind but catching up
  - the attack model is better understood
  - at least enforce the requirement of a per-vehicle physical contact (avoid Internet-style hacking of classes of vehicles)
- ITS is a required step towards fully automated driving

# Literature

- Used in this presentation (a.o.):
  - 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
- Documentation from recent EU projects
  - e.g. Converge
  - DG Mobility and Transport