

**Part I**  
**Security Challenges in**  
**Automotive**  
**Hardware/Software**  
**Architecture Design**

***Martin Lukaszewycz***  
***TUM CREATE Singapore***

Motivation (current E/E architectures)

Trends (Integrated Architectures / Connected Car)

Challenges Overview

Example CAN Bus

Challenges Electric Vehicles

**ZDNet** Search ZDNet

Hot Topics Newsletters Reviews Downloads White Papers Log In | Join ZDNet

Asia Edition SaaS Security Apps India CXO Telcos Startups Singapore SMBs Smartphones Cloud

MUST READ: iPad 5 features that are coming your way

Topic: Security Follow via: RSS Email

## Hackers steal keyless BMW in under 3 minutes (video)

**Summary:** *It's cool to have a keyless BMW, until you no longer have a keyless BMW. Hackers have figured out how to break into such cars with ease. BMW has acknowledged there is a problem, but is not doing enough to protect its customers.*

By Emil Protalinski for Zero Day | July 9, 2012 -- 18:29 GMT (20:29 CEST)  
Follow @emilprotalinski

Stolen BMW 1M Coupe in less than 3 minutes

ZDNet Follow @zdnet Like 142k Join | Log In | Privacy | Cookies

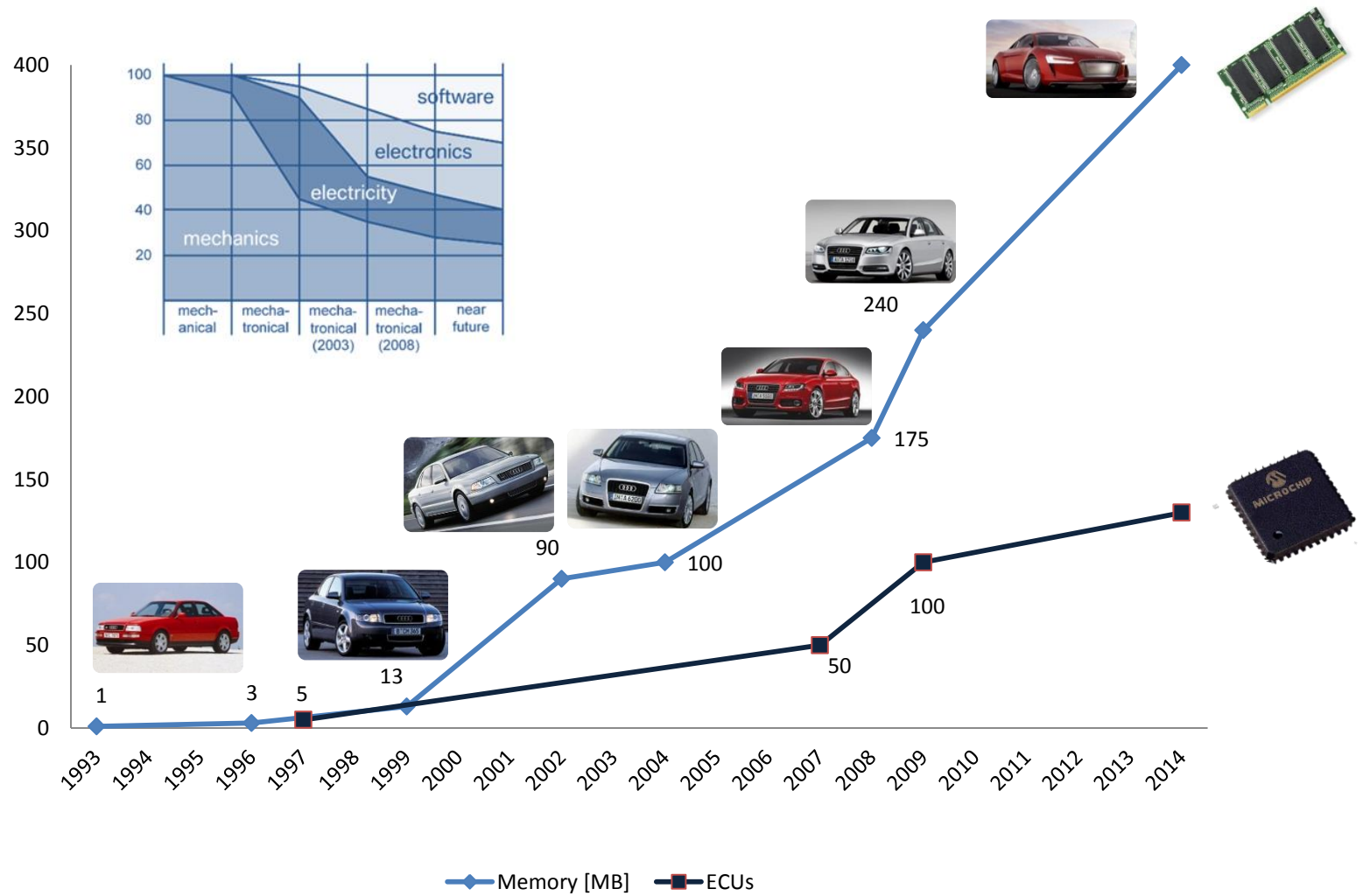
### Related Stories

- Welcome to bullyware: Malware gets more aggressive in money hunt
- Anonymous State of the Union threat is official: What you should know
- S'pore gallium nitride research linked to US engineer's death
- Anonymous hacks US Sentencing Commission, distributes files

### Resource Centre

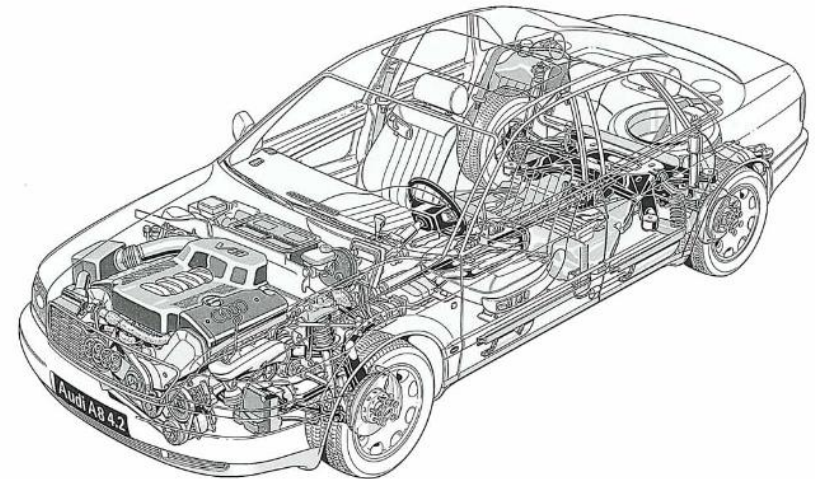
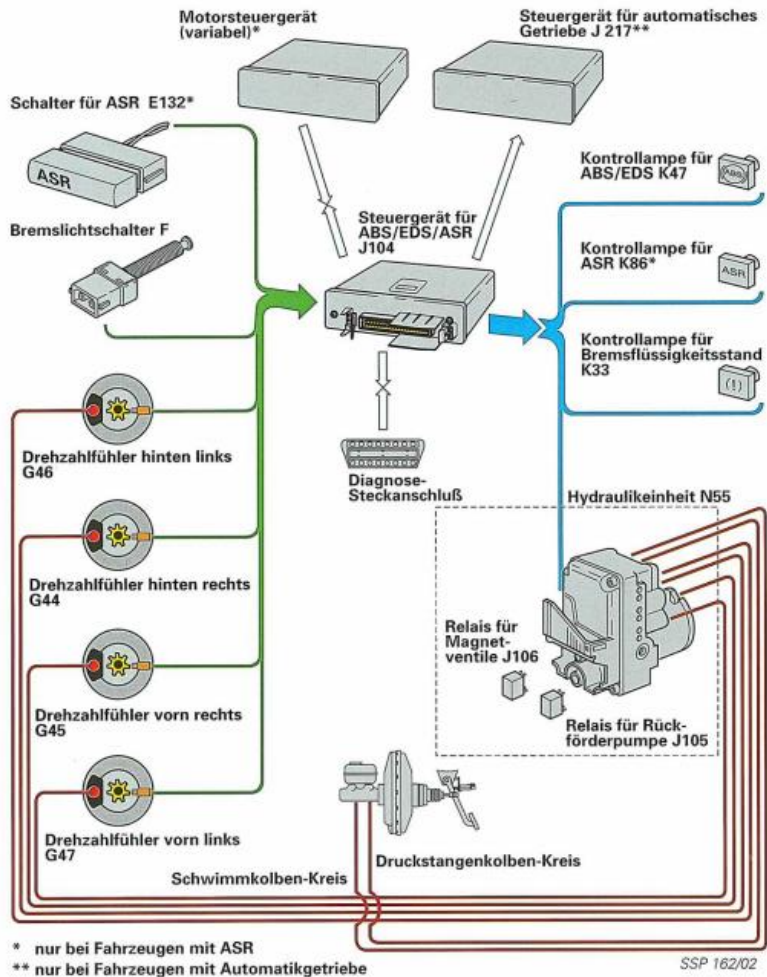
Useful content from our premier sponsors

# Increasing Complexity in Automotive Electronics



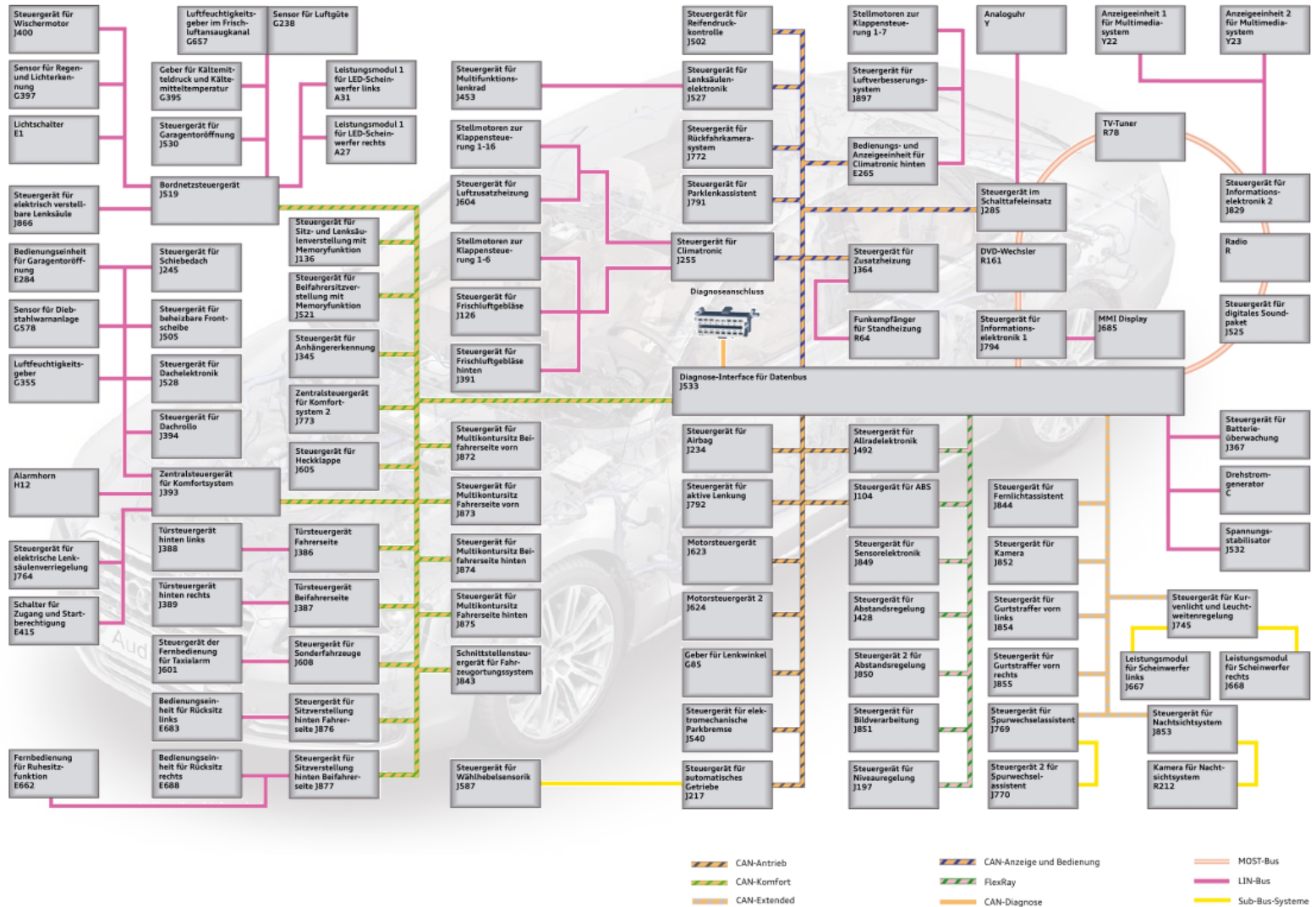
Sources:  
 Paul Milbredt, AUDI AG, EFTA 2010 - Switched FlexRay: Increasing the Effective Bandwidth and Safety of FlexRay Networks  
 BMW Group, FTF 2010 Orlando - Energy Saving Strategies in Future Automotive E/E Architectures

# Audi A8 - 1994



Source: Selbststudienprogramm - Audi A8 Audi ABS/EDS/ASR (Bosch)

# Audi A8 - 2010



Source: Selbststudienprogramm - Audi A8 '10 Bordnetz und Vernetzung

## OEMs

BMW, Volkswagen, General Motors,  
Toyota, Daimler



## Tier 1

Bosch, Continental, Delphi, Denso



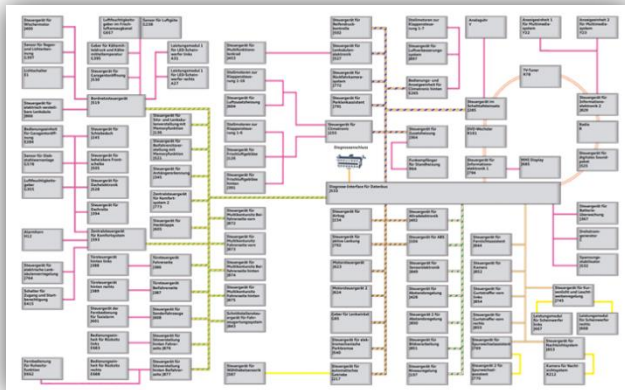
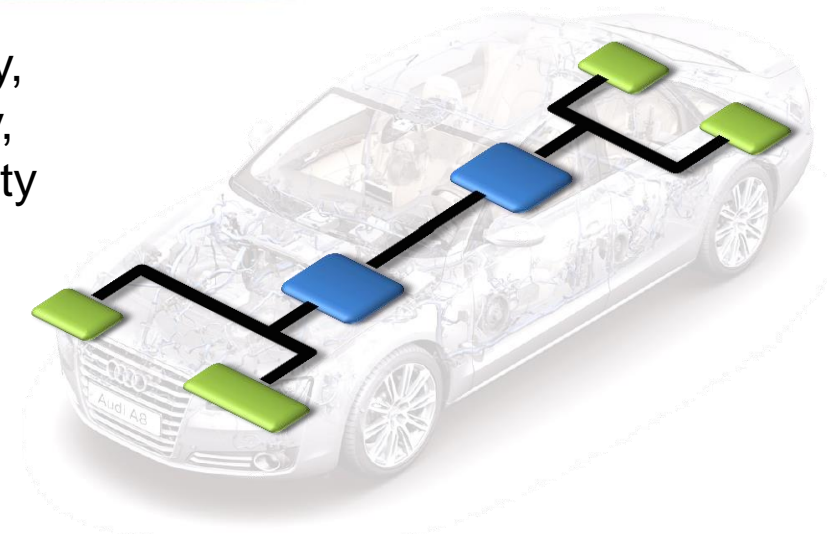
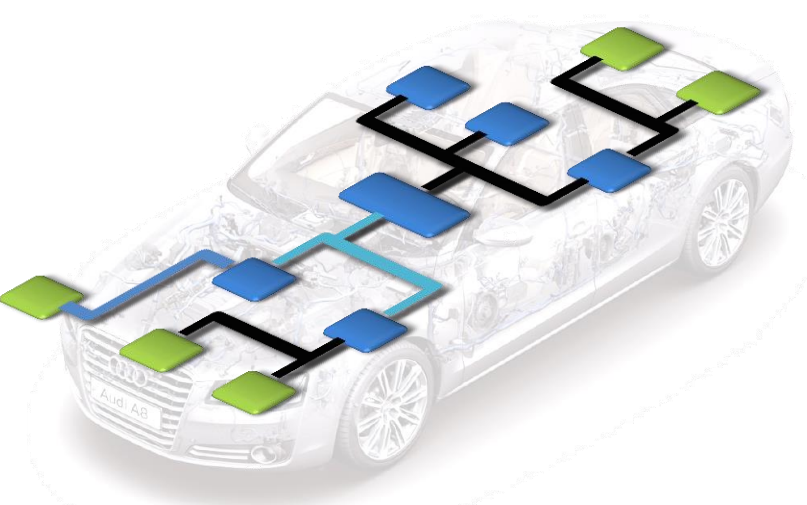
## Tier 2

Infineon, NXP, Freescale, Renesas



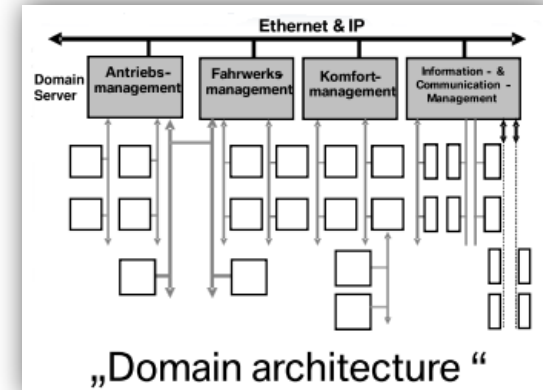
# Trend 1: From Federated to Integrated Architectures

Costs:  
Scalability,  
Flexibility,  
Extensibility



**State-of-the-art E/E Architecture**

Source: Selbststudienprogramm - Audi A8 '10 Bordnetz und Vernetzung

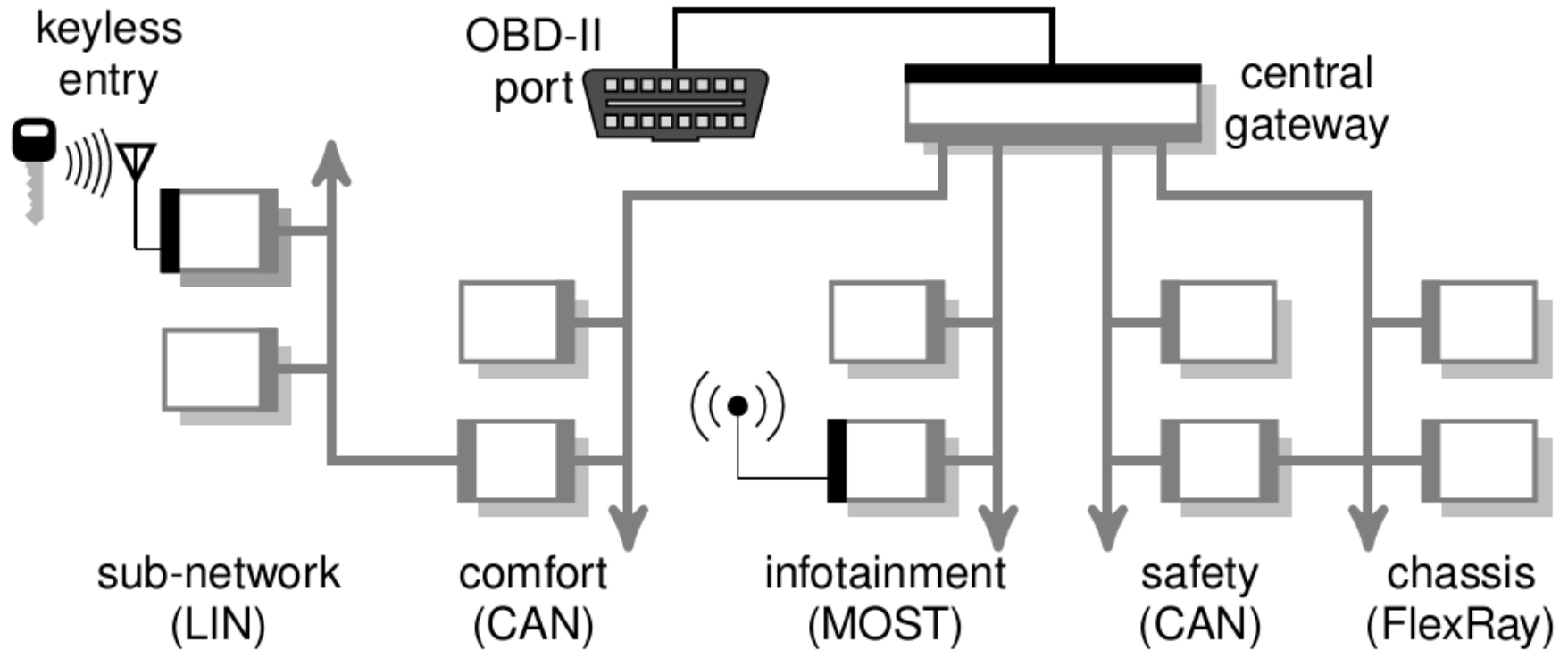


**Domain Architecture Concept from BMW**

Source: Ethernet for Automotive Applications. Robert Bruckmeier. Freescale Technology Forum, Orlando. June 23, 2010.



# In-vehicle network today / Access points



# Trend 2: Connected Car



Audi AG – Audi Connect

Available on the Audi App Store  
Apple Inc.

# Top Ten Most-Destructive Computer Viruses

Source: <http://www.smithsonianmag.com/science-nature/Top-Ten-Most-Destructive-Computer-Viruses.html>

- 1) Stuxnet (2009-2010)
- 2) Conficker Virus (2009)
- 3) agent.btz (2008)
- 4) Zeus (2007)
- 5) PoisonIvy (2005)
- 6) MyDoom (2004)
- 7) Fizzer (2003)
- 8) Slammer (2003)
- 9) Code Red (2001)
- 10) Love Letter/I LOVE YOU (2000)

# Automotive Design Objectives



Safety



Costs

Vs.



Security

Security issues in vehicles can lead to fatal consequences.



# Challenges: Security issues in automobile

## Wireless connectivity



## Malicious software



[www.computer-automation.de](http://www.computer-automation.de)

## Unauthorized products



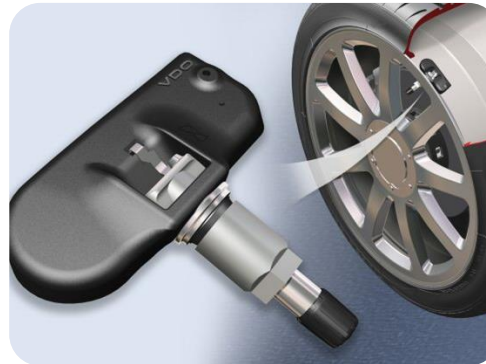
[www.bhptuning.de](http://www.bhptuning.de)

## Accessible buses/ECUs



[westseattleblog.com](http://westseattleblog.com)

## Unprotected sensors



VDO

## Counterfeits

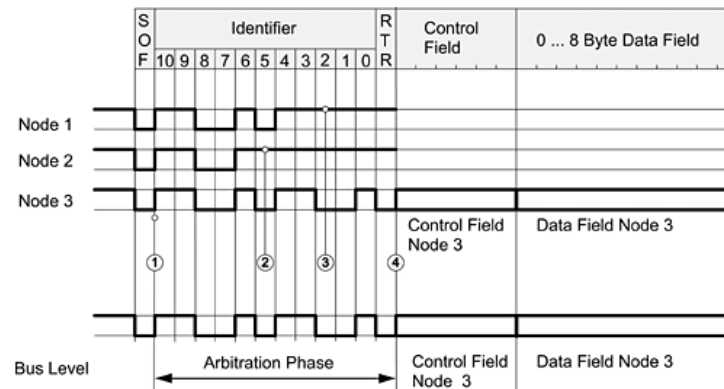


[shoebossion.wordpress.com](http://shoebossion.wordpress.com)

# More than two billion CAN nodes have been sold since the protocol's development in the early 1980s.

Source: D. Wrangler Security Threats and Countermeasures for Intra-vehicle Networks

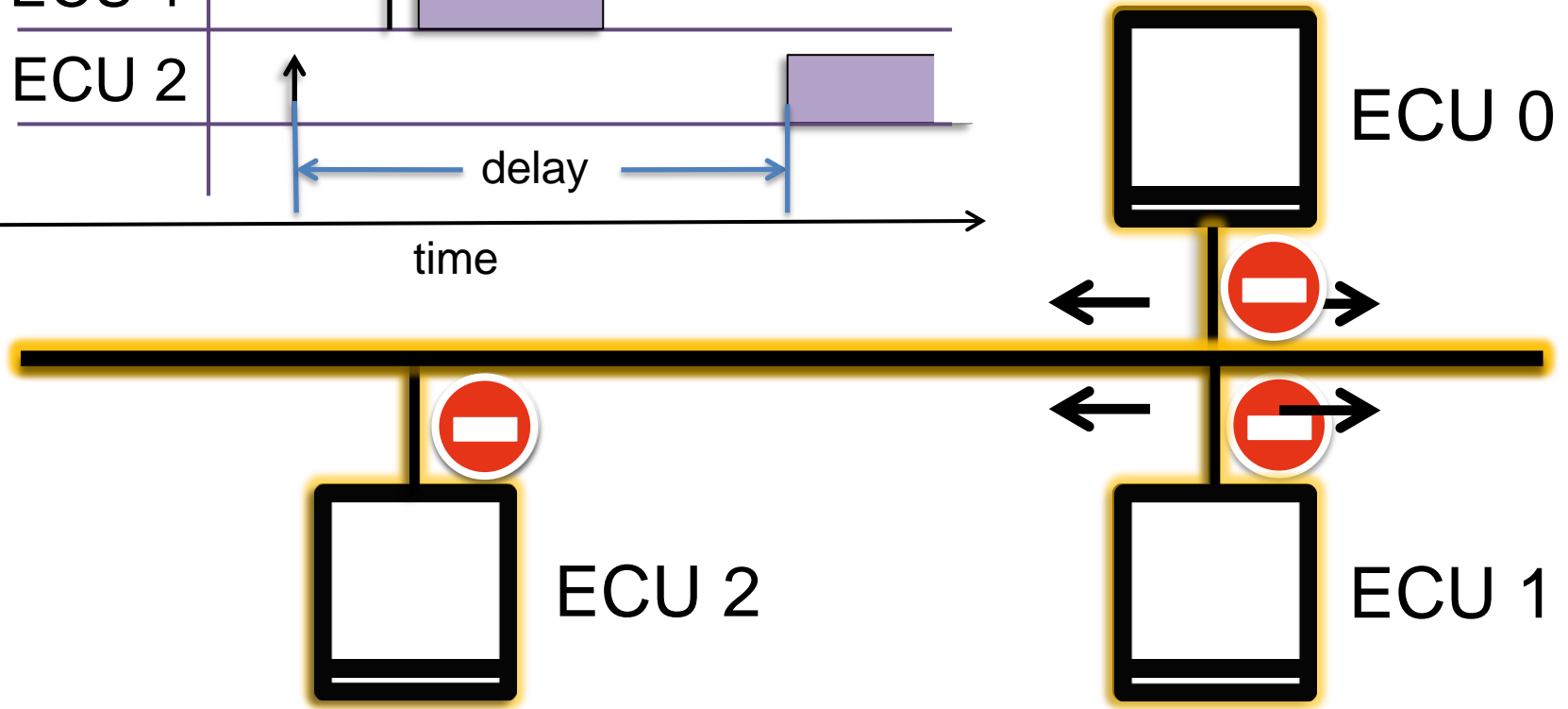
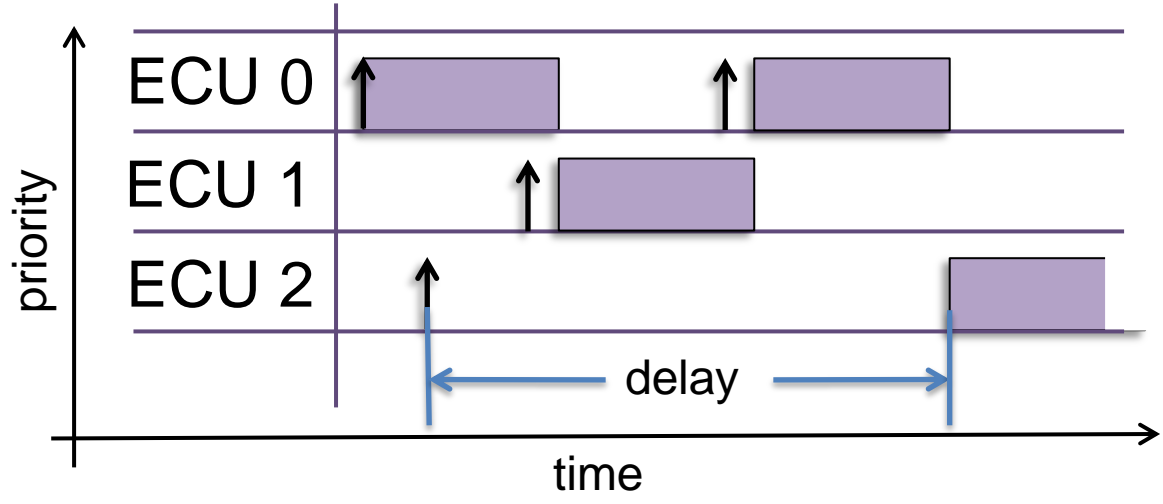
# CAN



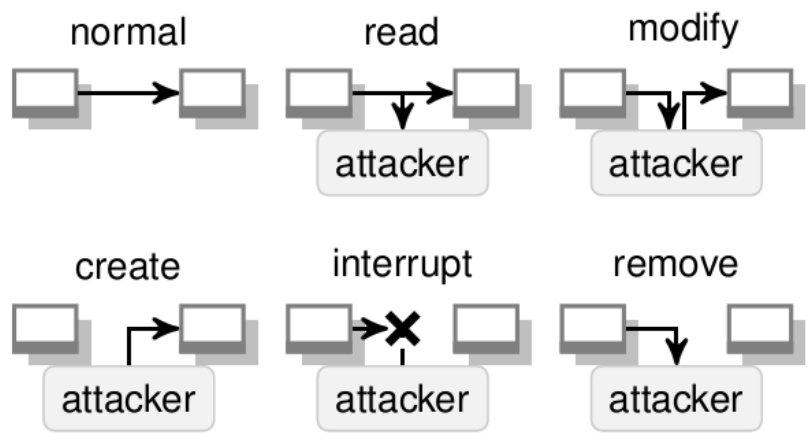
Source:  
[http://www.ixxat.com/can-controller-area-network-introduction\\_en.html](http://www.ixxat.com/can-controller-area-network-introduction_en.html)

# CAN bus operation

# CAN

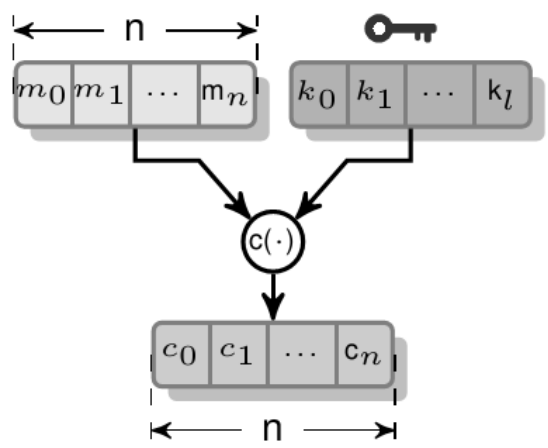


# CAN vs Secure communication

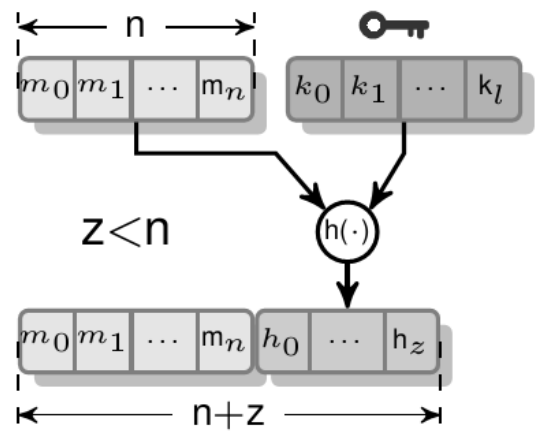


violated principle	read	modify	create	interrupt	remove
<b>confidentiality</b>	X	X			
<b>integrity</b>		X	X		
<b>availability</b>				X	X

## Message encryption:

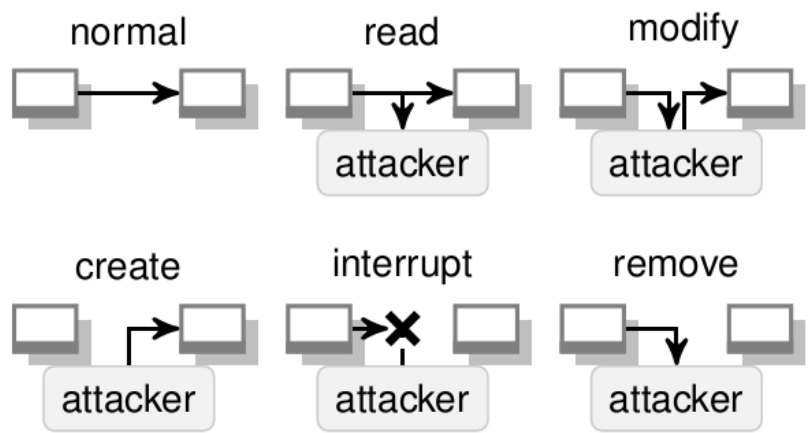


## Message authentication:





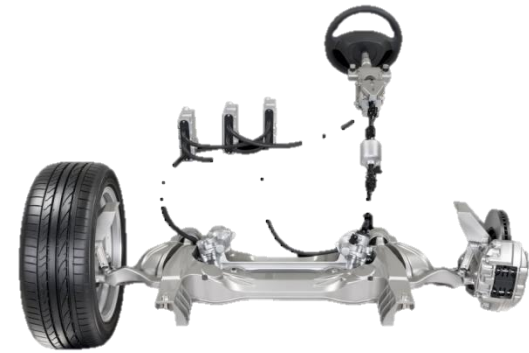
# CAN vs Secure communication



violated principle	read	modify	create	interrupt	remove
<b>confidentiality</b>	X	X			
<b>integrity</b>		X	X		
<b>availability</b>				X	X

	CAN	FlexRay	Ethernet
confidentiality	feasible	feasible	Available (IPSEC)
integrity	- ( only 8byte)	feasible	Available (IPSEC)
availability	- (Event-Triggered)	Available (Time-Tiggered protocol + Bus guardian)	Feasible (PTP + switches: bus guardian possible )

## Drive-by-wire

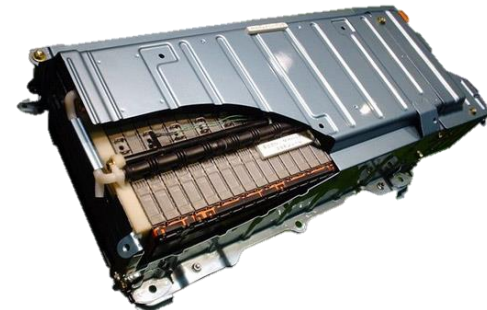


Nissan Drive-by-wire

## Charging plug

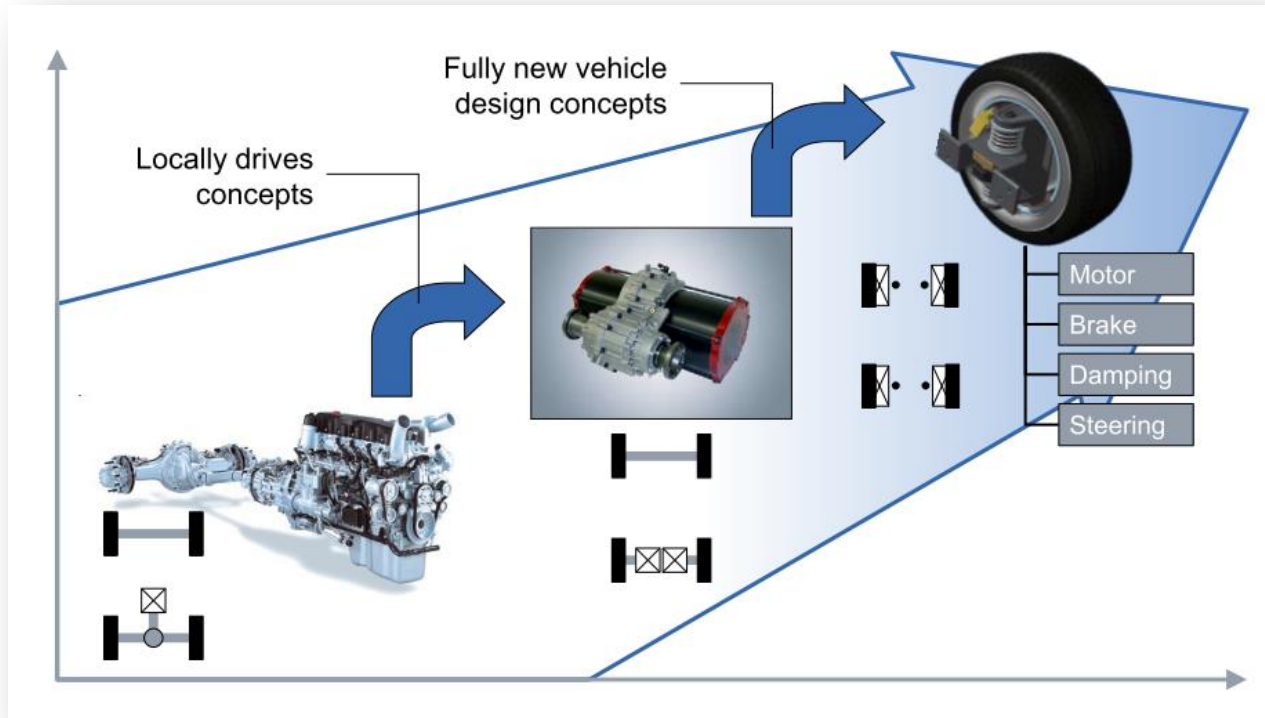


## Battery



## Energy-efficient recuperation

## Enabler of new drive-train architectures

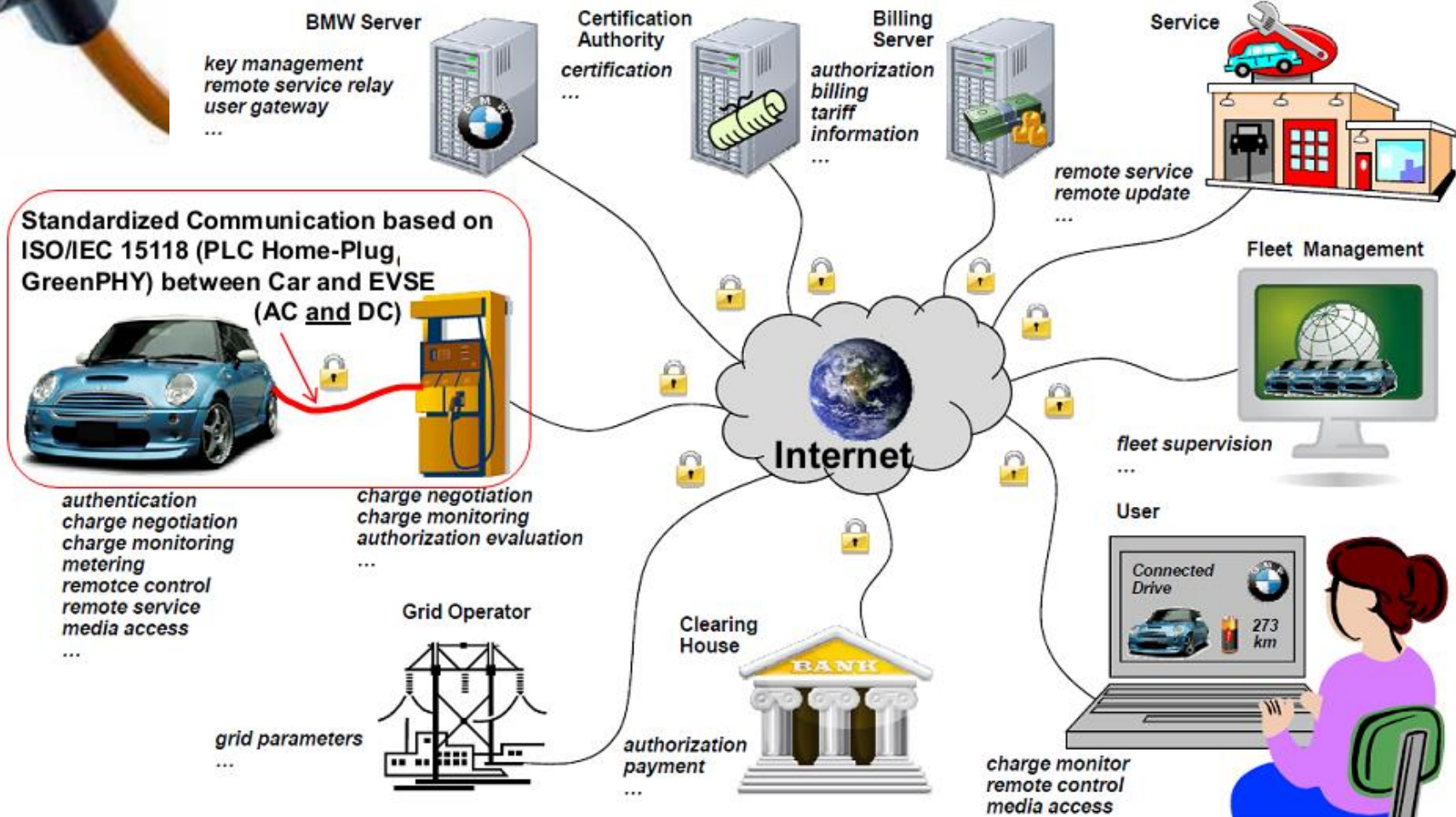


Source: Gunter Freitag, Eine zukunftsfähige E/E-Architektur für PKW

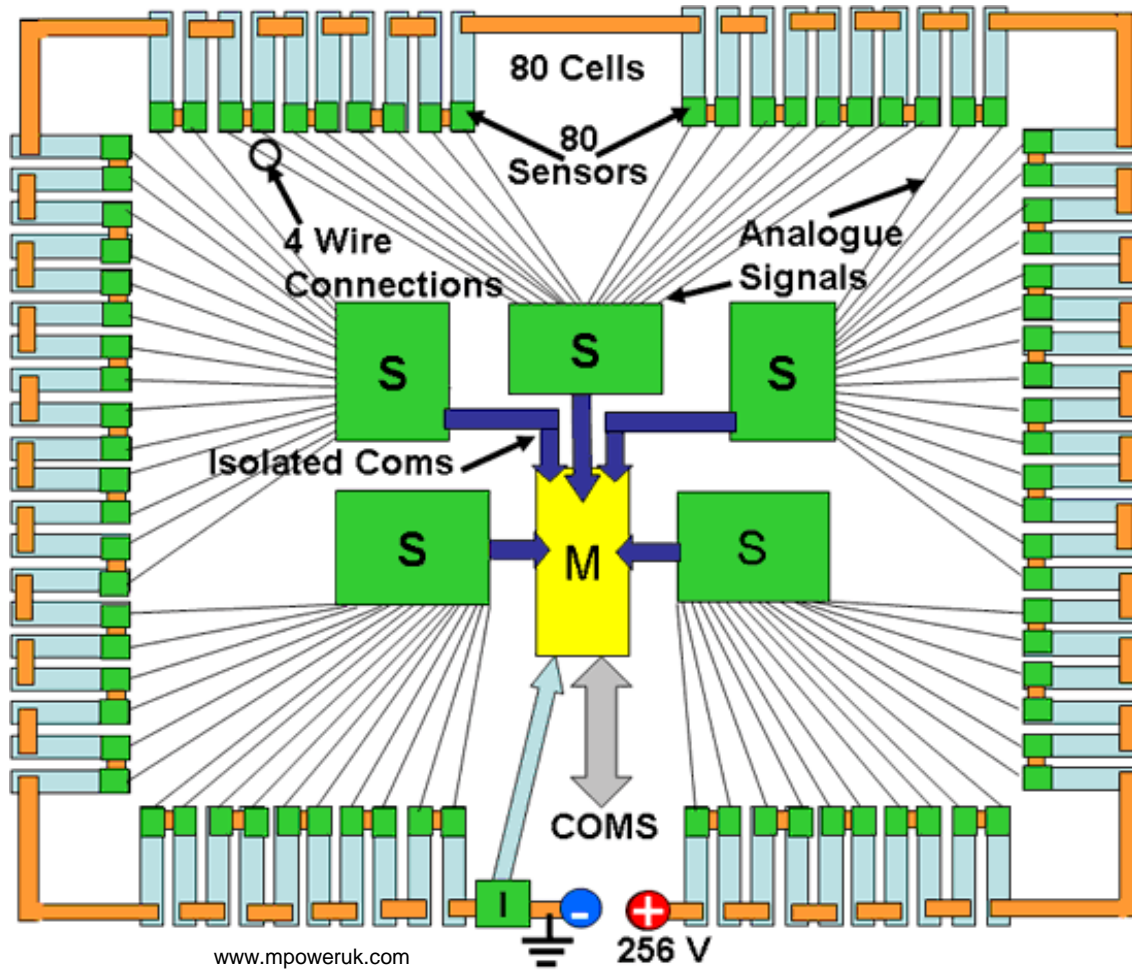
# Vehicle-to-grid / Charging plug



## ISO/IEC 15118:



# Battery Management



Monitors:



temperature

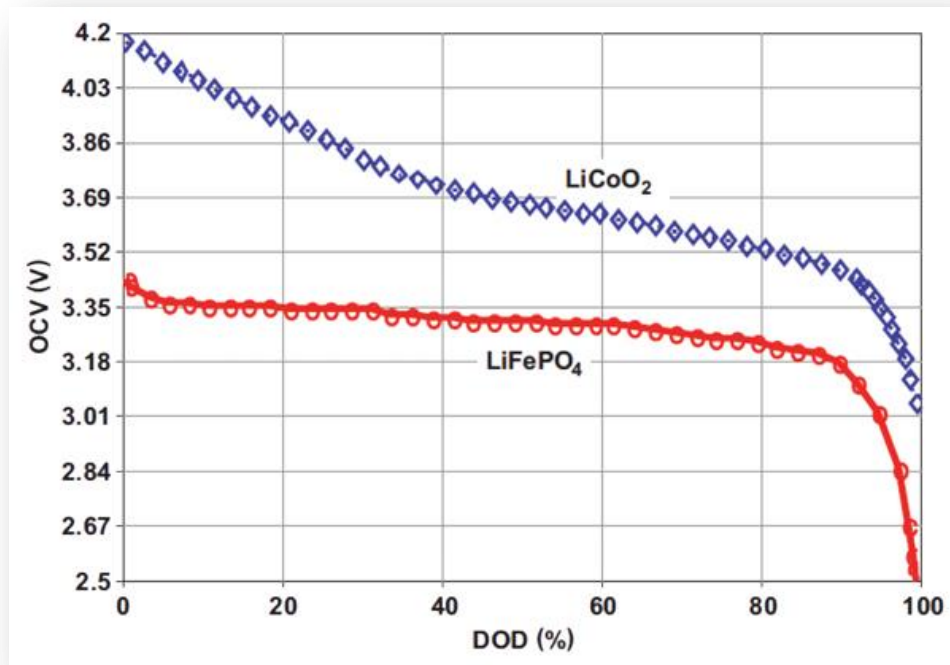


voltage



current


Battery cells have to be operated in a safe range



Source: <http://www.digikey.com/us/en/techzone/energy-harvesting/resources/articles/battery-fuel-gauges.html>

## Battery Safety





Thank you for your attention.  
Questions?