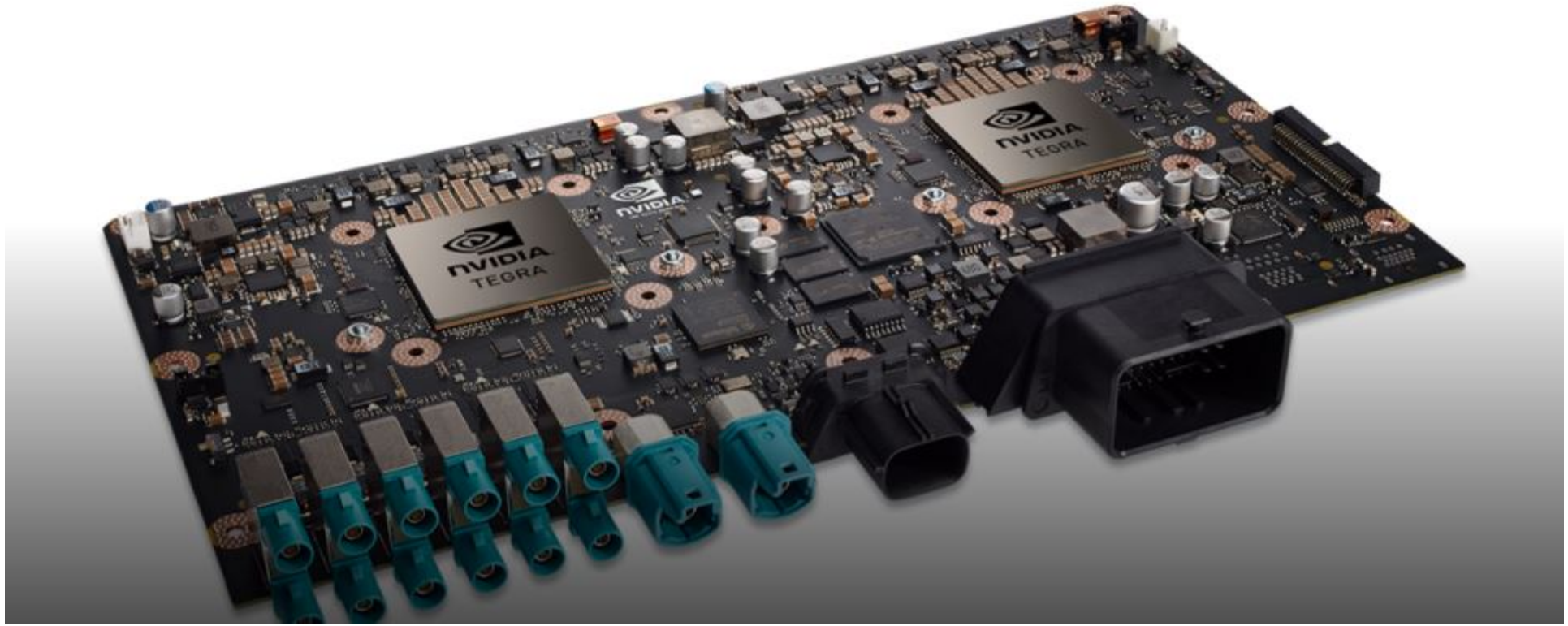
Electronic systems in modern cars

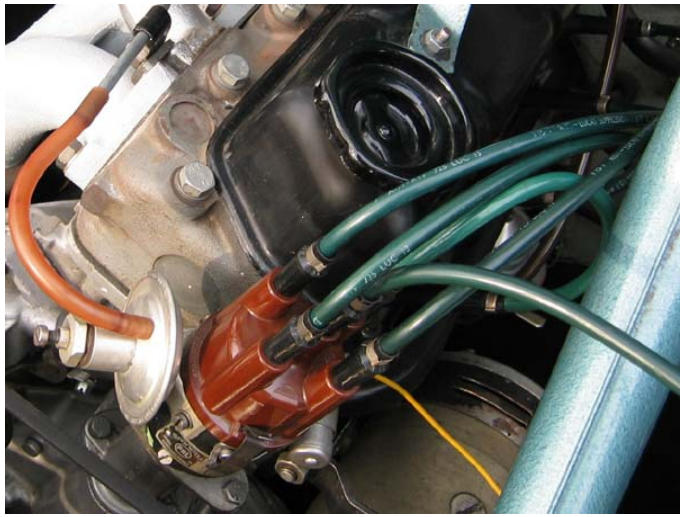


About me

- Working @ Trend Micro
- security researcher
- Focus on IoT and car security

Car electronics evolution

- Switches, wires, bulbs, mechanical ignition timing (analog signals i.e. coolant temp)
- Engine ECU – fuel injection, electronic ignition (still analog signals)
- Safety requirements – airbags, ABS, ESP
- Distributed controller architecture
- Digital communication between modules needed (CAN-BUS)
- Additional assistants – adaptive cruise control, park assist, lane change warning – faster and more reliable bus needed (FlexRay)
- Multimedia, NAVI, connected cars – high bandwidth (MOST and ethernet)



Wiring harness

- Straight wire analog topology (i.e. battery – fuse – switch – bulb)
- Current can be high – thick wires
- With increasing number of devices wires become
  - heavy
  - expensive
  - unreliable
- Switch can be connected to a controller by thin wire
- Today multiple switches are connected by LIN bus to a controller

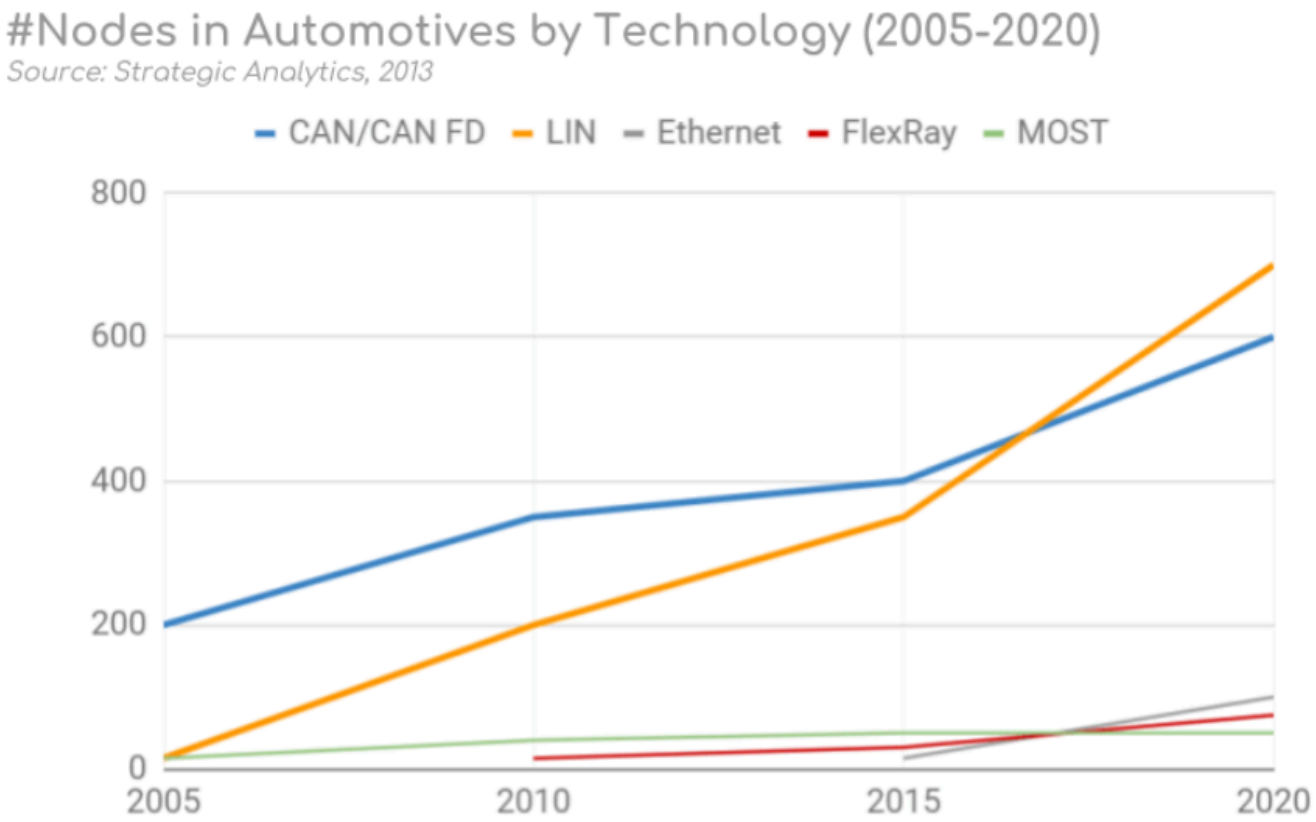
Example - headlight

- Straight wire – simple on/off switch function, 2x 55W + 2x 10W bulbs @ 12V draws about 10A -> with 5% acceptable loss 4 mm^2 wire is needed
- With headlight embedded controller 10 mA control signal is enough -> 0.25 mm^2 wire can be used
- Additional benefits – soft start circuit, diagnostic function (light source failure)

Interconnection evolution

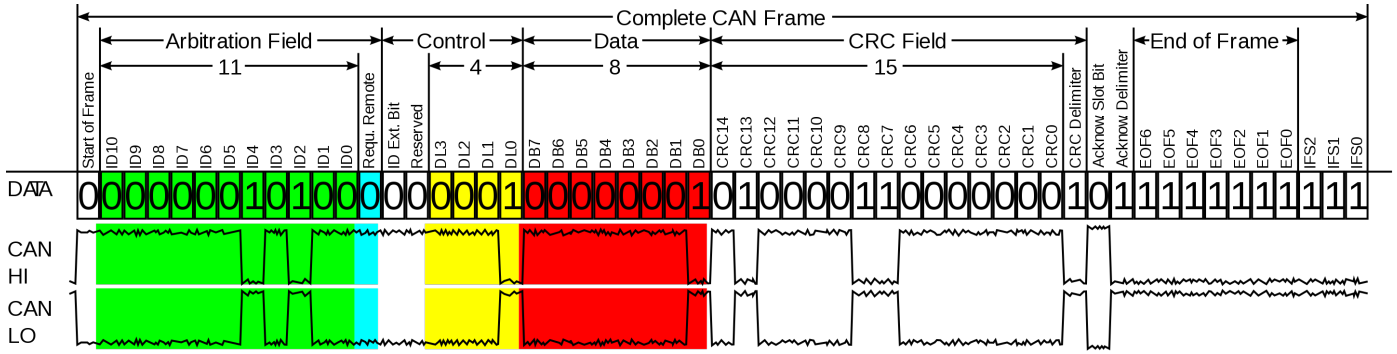
- Distributed controller achitecture
- With growing number of ECU a lot of real-time info must be distributed between them
- Digital bus technology was used to connect ECUs – CAN
- CAN bandwith is 40kb to 1Mb
- initially bandwith was sufficient for data interchange (usually 1-M)
- Internal car status data x external sensors (imaging) data
- There was need for large data transfers (multimedia, navigation, firmware) -> higher bandwith techology (MOST, ether)
- For critical functions (X-by-wire) collision protocol is not suitable
- Guaranteed transfer time is needed – FlexRay

Automotive bus technology adoption



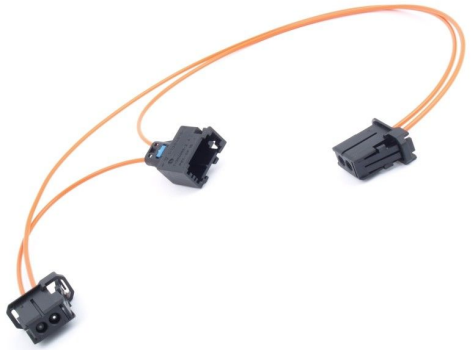
CAN

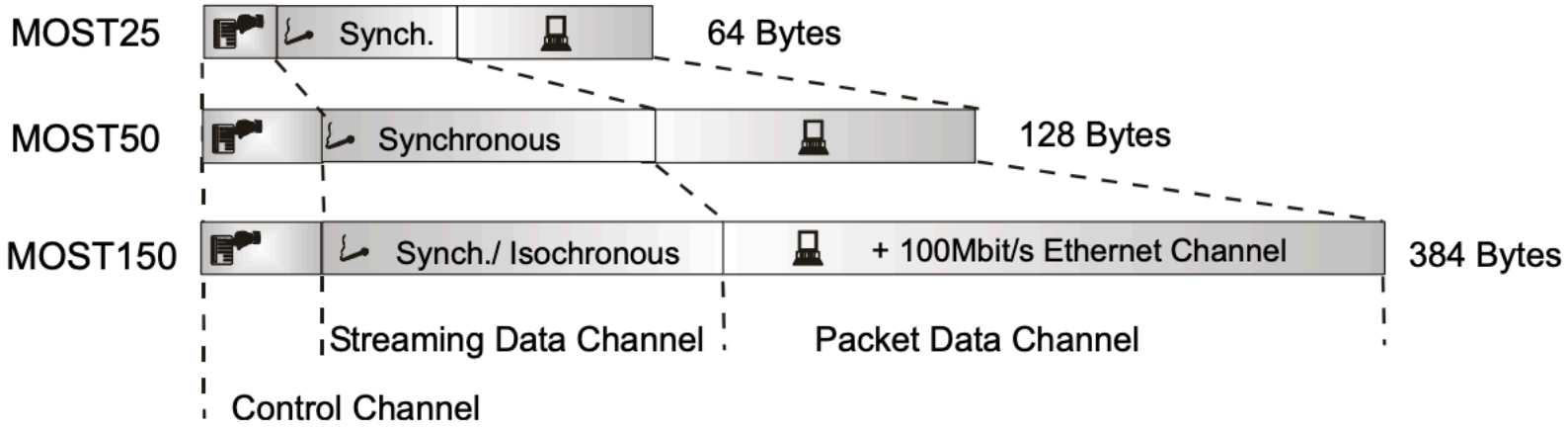
- Developed by Bosch in 1983-1986
- First commercial use in 1991 – MB W140
- Robust (differential twisted wires, CRC, low speed)
- Media sharing protocol, message based, bit stuffing (synchronization)
- ID defines priority in case of collision (rev A: 11 bits, rev B:29 bits)
- Must be terminated (120 ohm), uses 0-5V levels
- ACK bit – needed to confirm reception of at least 1 node
- Error counters : TEC, REC
- Node error state (passive err, active err, bus off)
- Error frame: active, passive
- Speed up to 1Mb (5Mb CAN-FD)



MOST

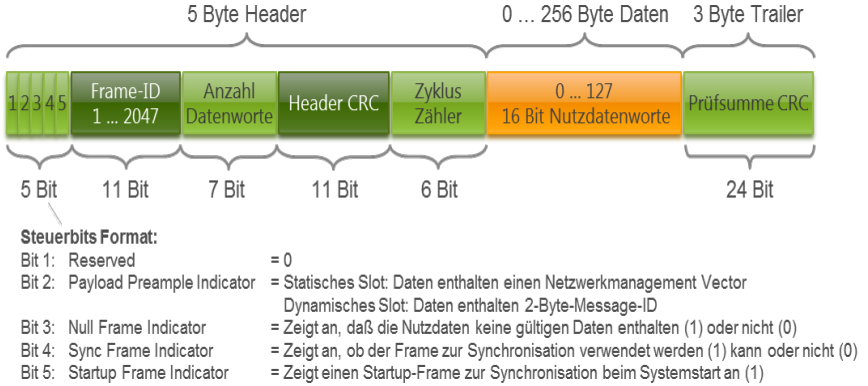
- Media Oriented Systems Transport
- Continuation of Daimler‘s D2B technology
- Developed since 1996 at BMW for media data transfer
- Usually optical fibre (1mm plastic fibre with red wavelength LED)
- Usually ring topology, master-slave timing
- Speed 25, 50, 150 Mb

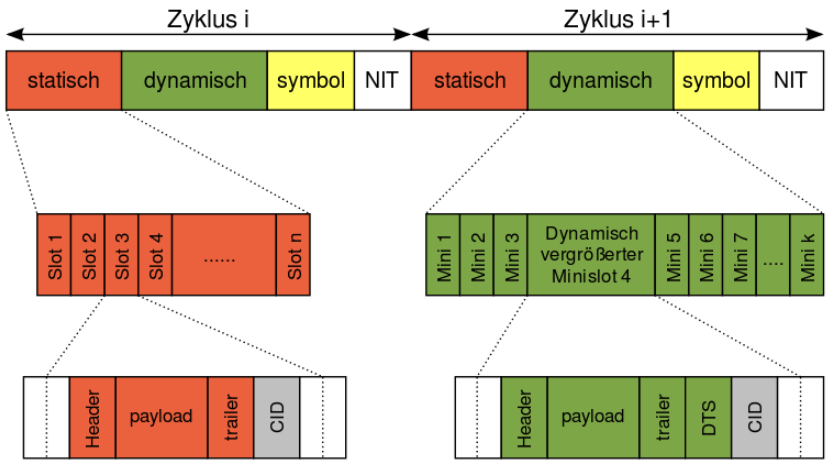




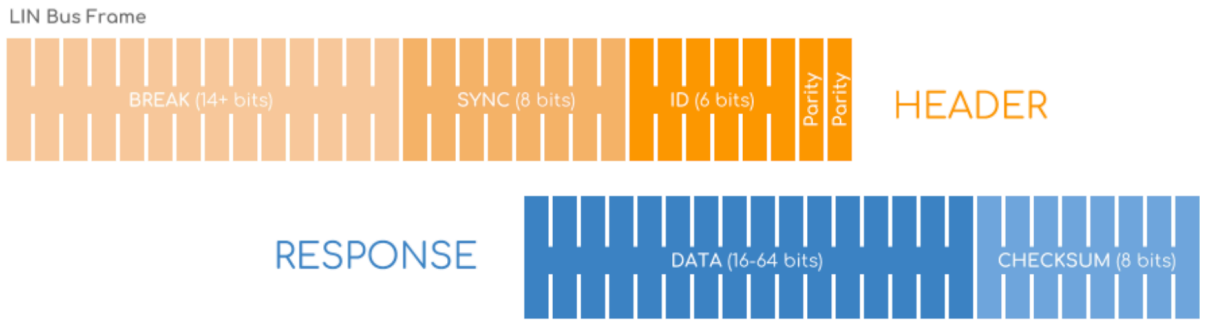
FlexRay

- For specific applications CAN is slow, cannnot guarantee delivery in time
- Flexray consortium was founded by BMW and Daimler in 2000
- Consortium was dismissed in 2009 but FlexRay become ISO standard
- First commercial usage in BMW X5 in 2006 for dynamic damping
- Max speed 10Mb
- Dedicated time slots – no collisions
- Expensive – used today for critical functions (steering, braking…)
- One channel uses 2 differential twisted pair. 1 or 2 channels can be used.
- Protocol is very complex and details are beyond scope of this presentation
- Development board costs over 1k USD.



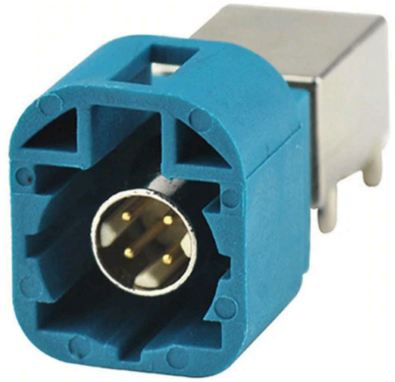


LIN



- CAN was expensive for simple applications like switches
- European automotive consortium released LIN in 2002
- Serial protocol, 1 wire, 12V signal
- Master-slave communication -> no collision
- Max 16 nodes
- Slave node position detection after power up
- Speed 19.2 kb
- 6 types of frames

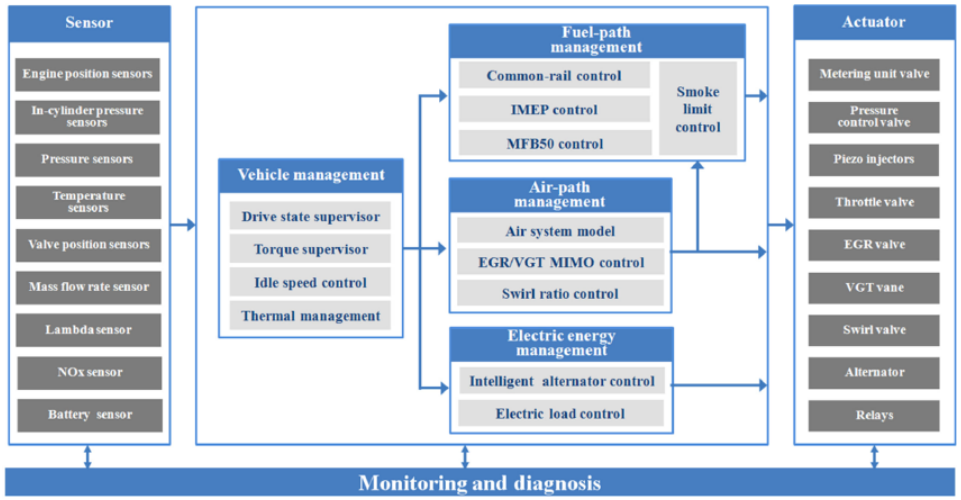
Ether



- 100TX Ethernet physical level standard is not suitable for automotive
- CAT5+ is expensive, RJ45 is not prone to vibrations, high EMI
- BroadR-Reach by Broadcom adopted as a standard in 2011
- Uses more sophisticated signaling (reducing signal bandwith and EMI)
- Simple unshielded twisted pair with FAKRA connectors

Engine control

- Initially needed for injection control (ignition timing, fuel amount)
- Engine management is very complex today (10ths of parameters are monitored realtime)
- Similar principles for petrol and diesel engines
- Engine ECU is managed by other systems (ESP, automatic transmission etc.)

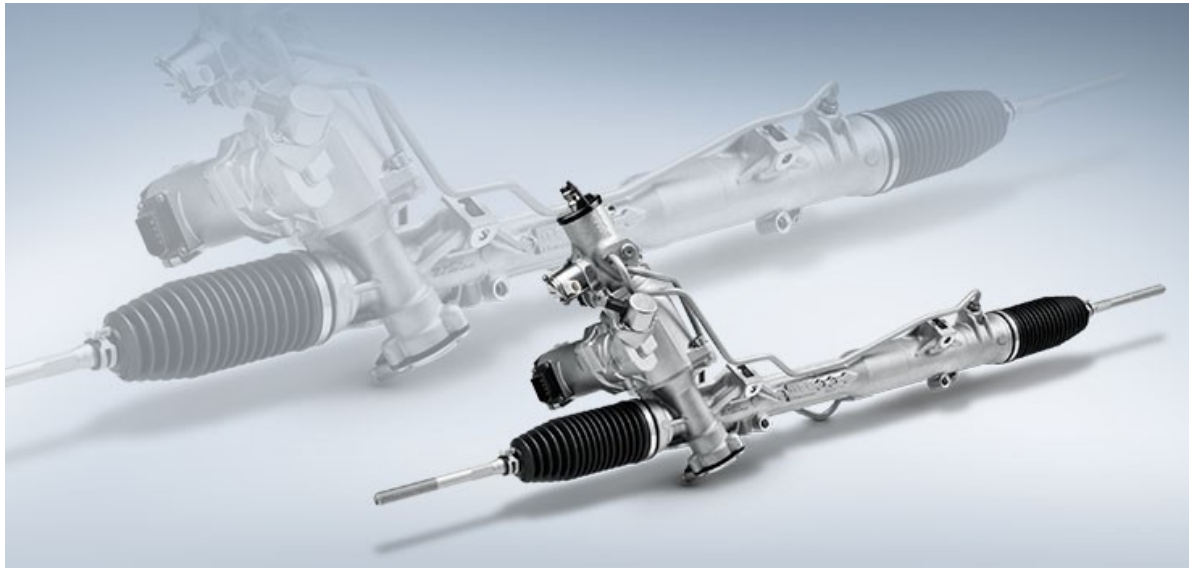


Instrument cluster

- Initially mechanical dial pointers, bulbs – basic state info
- Stepper motors, LED, LCD – advanced state info
- Full size TFT displays + HUD – online multimedia, navigation data

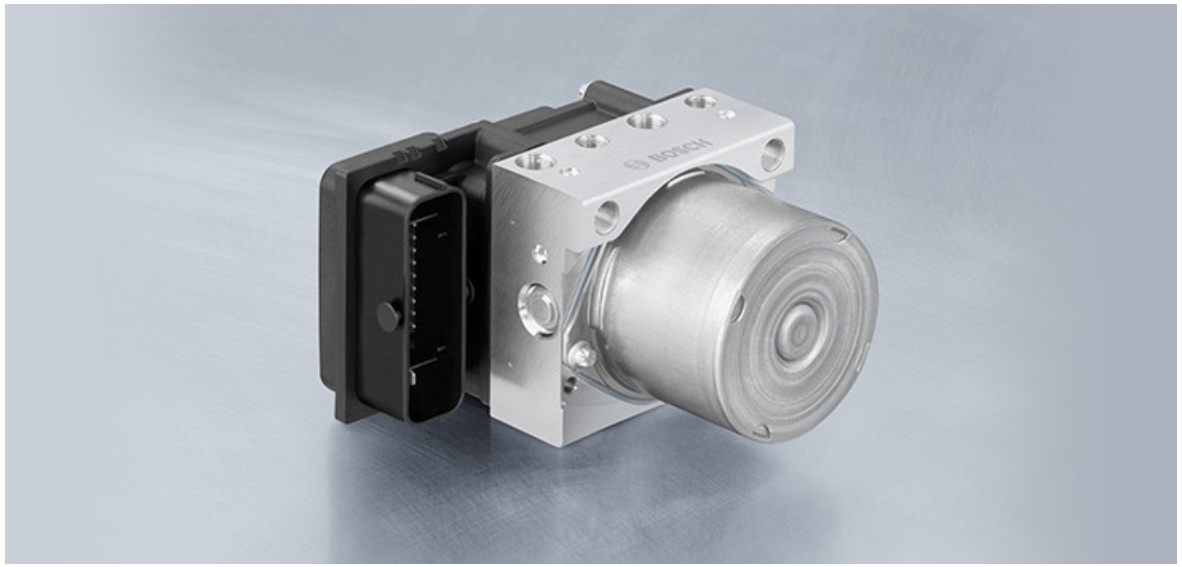
Power assisted steering

- Increases steering forces to ease steering
- Initially hydraulic, later electric
- Supporting forces can be degressive (with increasing speed)
- can be actively used in park assist or autonomous steering
- Drive-by-wire (steering wheel not mechanically linked to wheels)



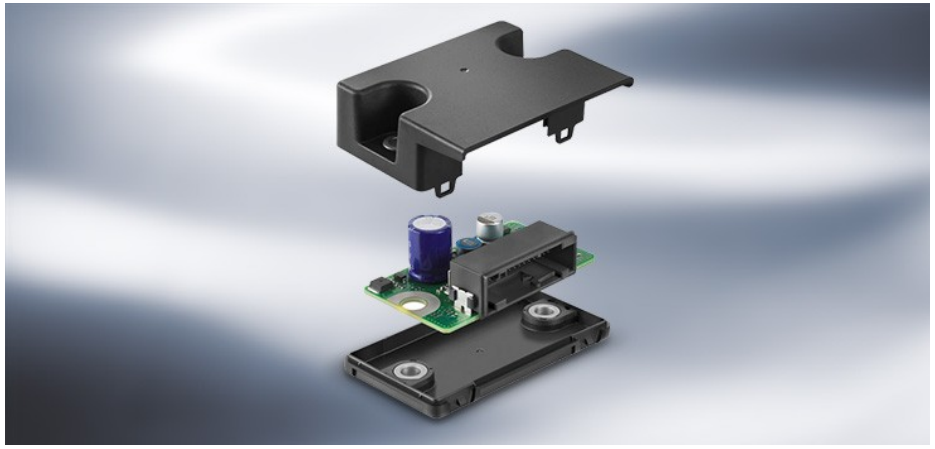
ABS

- First security assistant – prevents traction loss during breaking
- Wheel speed sensors
- Modulate breaking fluid pressure to individual wheels



Security restriction system

- Airbags
- Seat belt tensioners
- Active headrests
- Multiple sensors (acceleration) to avoid false activation
- Fault tolerant (multiple µC, multiple SW)
- Independent power supply
- Crash data recorder

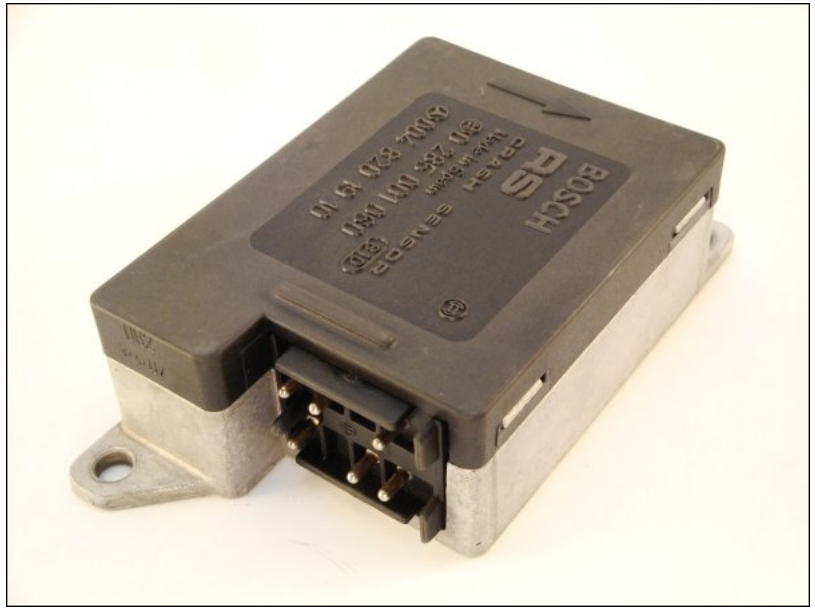


Airbag unit controller

- Responsible for restriction devices deployment
- Have enough energy even in case of power loss
- ISO26262 / ASIL D requirement: to have 2 uControllers and at least 2 accelerometer sensors for redundancy
- Bosch (> 80%) and Continental are leaders in production and development

Bosch airbag unit history

- first generation of airbag ECU had 170 parts in 3 components controlling just one airbag (driver) and was introduced in 1981 in MB S-class
- AB 9 in 2003
- AB 10 in 2005 (85 parts in 1 component) for up to 24 restraint devices, manufacturing started in 2007.
- Units AB 12 (AB base) and AB 12+ (AB enhanced) were introduced in 2015



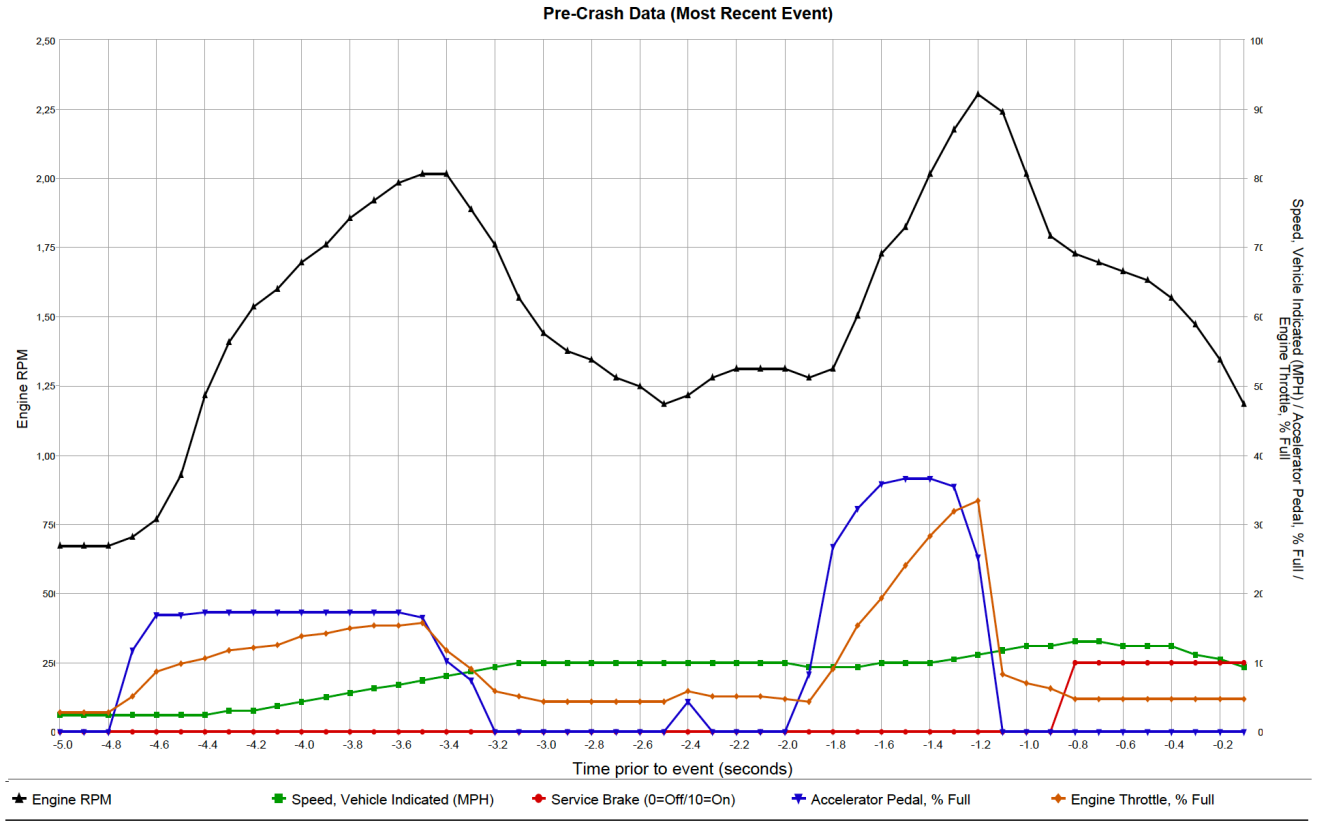
CDR

- Crash Device Recorder – records last several seconds (5-12 usually) before crash
- Allows advanced crash analysis, even if one car only is equipped with CDR
- Insurance, law enforcement of private investigators can have tools (i.e. Bosch CDR 900 for 4k USD)
- All cars manufactured after 2013 and most produced after 2005 have CDR (US&EU law enforcement)

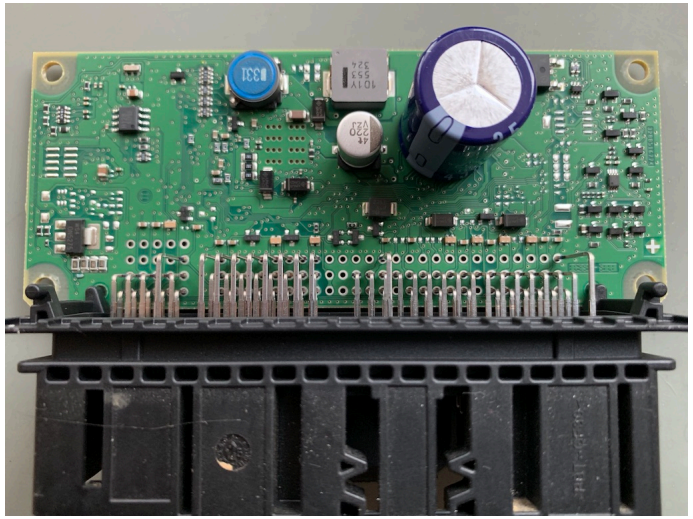
CDR report

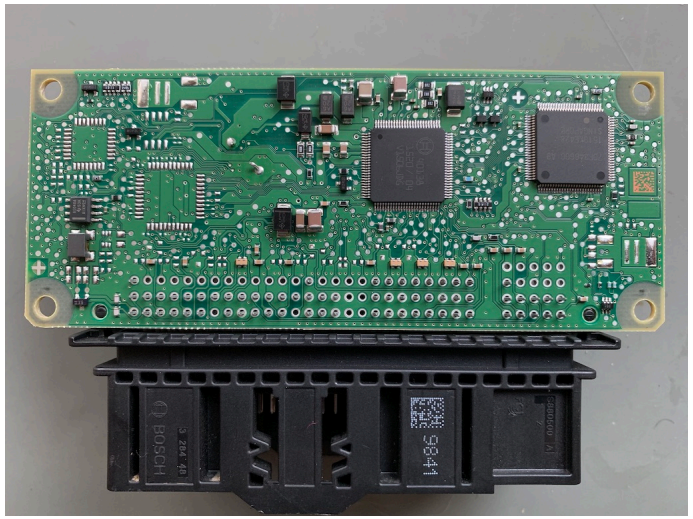
- ~ 27 pages
- Info about (in ms samples):
  - ✓vehicle speed
  - ✓engine RPM
  - ✓ accelerometer value
  - ✓ steering angle
  - ✓ brake pressure
  - ✓gas % values
  - ✓seatbelt usage
  - ✓etc.

BOSCH

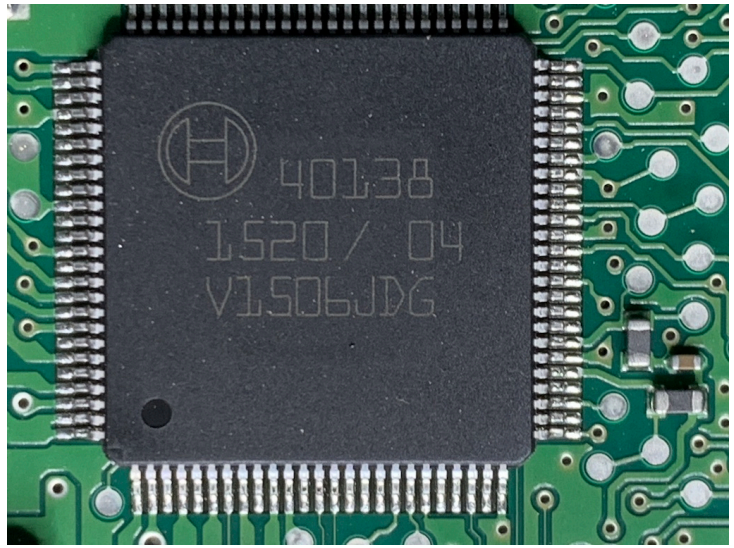


Example: BMW ACSM



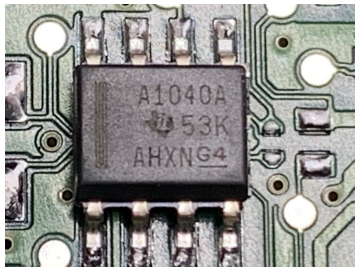


Controllers



BOSCH 40138: ECU IC Airbag Computer Driver Chip

70F3464GC NEC V850E/RG3 32 bit microcontroller
User's and architecture manual are available

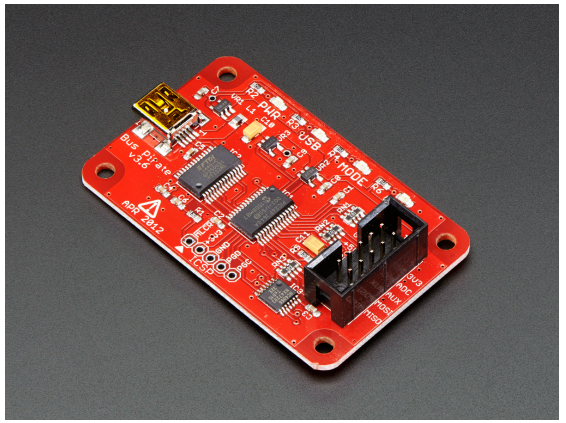


TI A1040A CAN bus controller

128kb EEPROM

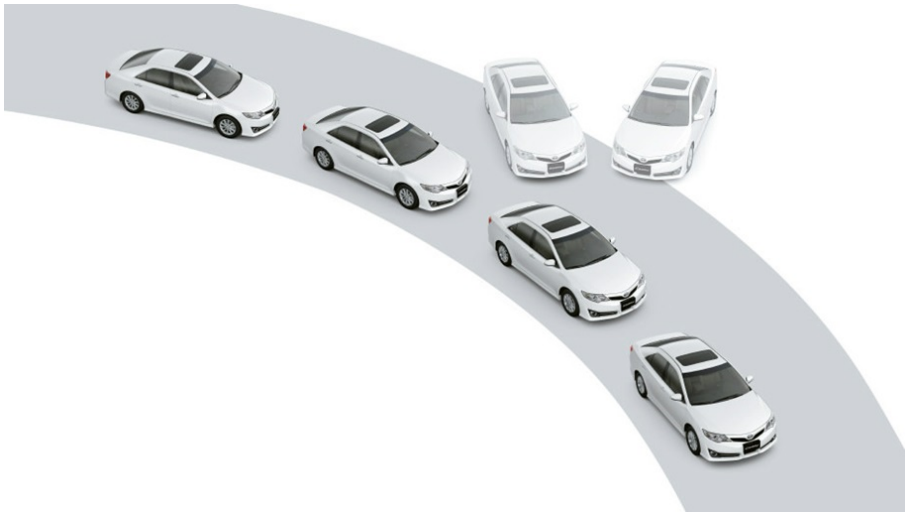
Hacking BMW airbag unit

- ECU bought on eBay from crashed car
- ACSM serves as CDR
- After crash it is unusable and must be replaced (oficially)
- FW reflash with BMW diagnostic tools doesn‘t help
- Crash data are stored in 128kbit EEPROM
- EEPROM could not be desoldered without damage
- Overwritten contents over SPI bus with BusPirate
- ACSM was initialized with diag tools afterwards



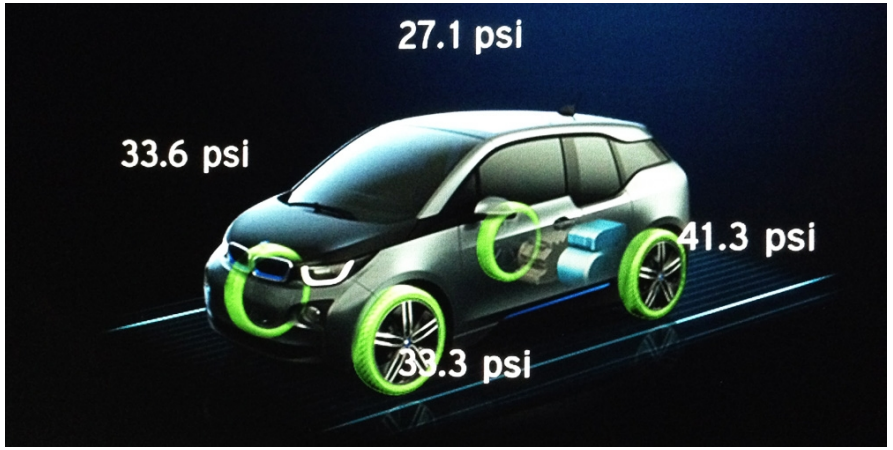
Traction and stability control

- Evolution of ABS systems
- Tries to avoid other uncontrollable situations
- Additional sensors
- Uses ABS hydraulic actuators, cooperates with other systems



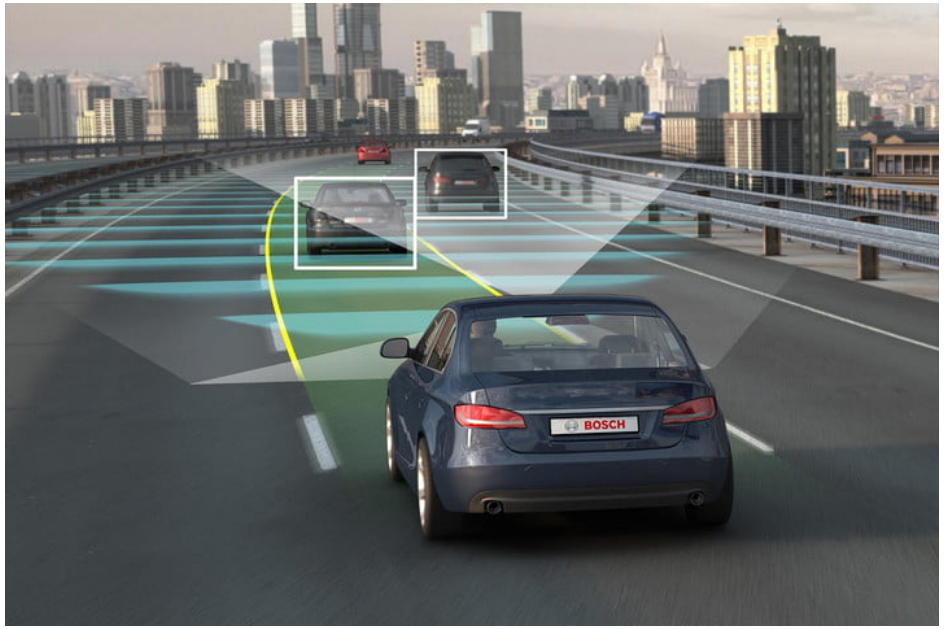
Tire pressure monitoring

- Important for stability control
- Indirect – wheel speed difference
- Direct – TPMS sensors – air pressure, temperature



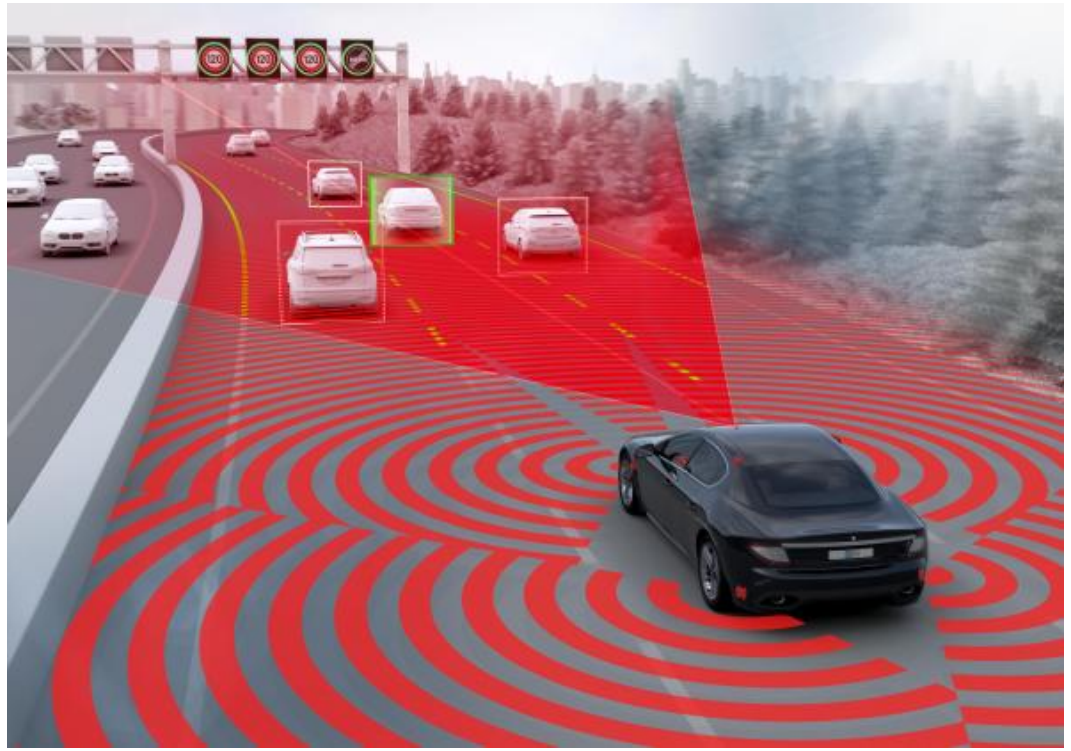
Cruise control

- Maintaining constant speed (part of engine ECU)
- Adaptive systems
  - need real time data about surrounding objects
  - radar, lidar, ultrasonic sensor, camera



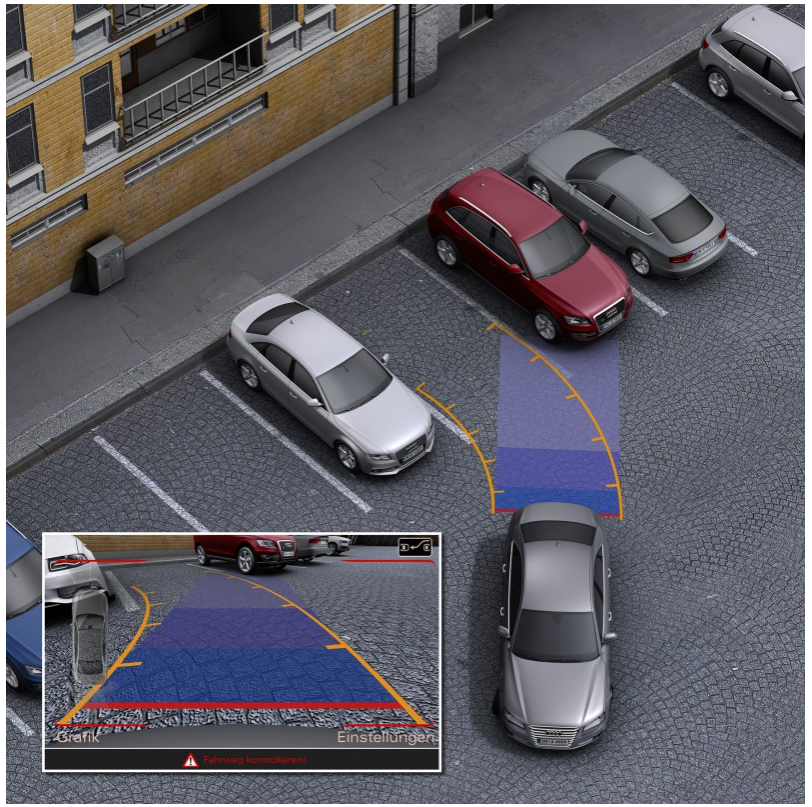
Lane change assistance

- Camera output image processing
- Other sensors – radars in vehicle corners
- Simple blind spot warning
- Lane departure warning
- Active lane change assistance



Park assist

- Ultrasonic sensors, audio signal, passive
- Cameras, TFT display - active steering



X-by-wire

- Gas – most cars today
- Steering
  - Parking assistants, autonomous steering systems
  - Steering wheel usually still not disconnected from wheels
- Brakes
  - parking brake is usually electronically controlled
  - hill launch assistant
  - brake pads drying
  - main brake valve is usually still not disconnected from brake pedal

Autonomous driving

- SAE classification:
  - L0. human driven
  - L1. hands on
  - L2. hands off
  - L3. eyes off
  - L4. mind off
  - L5. human free