Bus Systems

Introduction

Prof. Dr. Reinhard Gotzhein, Dr. Thomas Kuhn

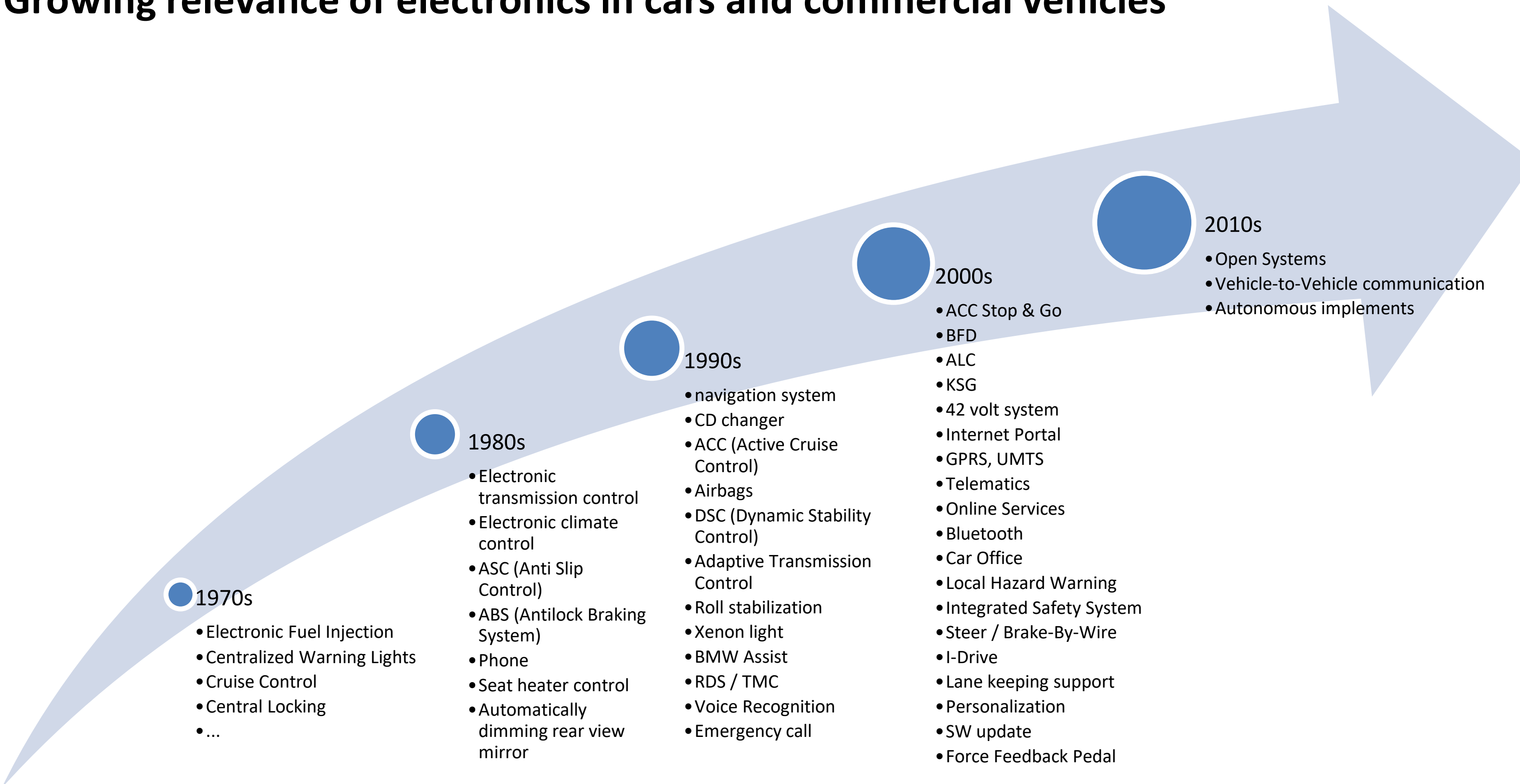
Introduction

Learning goals of this section

- Bus systems overview
  - Relevance of bus systems
  - Application areas of bus systems
  - Types of bus systems
- Automotive and commercial vehicle bus systems
  - Evolution of automotive networks
  - Automotive network topologies
  - Bus systems in commercial vehicles
- Safe communication
  - Safe communication needs
  - Predictable communication

Introduction

Growing relevance of electronics in cars and commercial vehicles



Adapted from: U. Weinmann: Anforderungen und Chancen automobilgerechter Softwareentwicklung, 3. EUROFORUM-Fachkonferenz, Stuttgart, Juli 2002

Introduction

History of vehicular bus systems

- Bus systems until the end of the 80s
  - Electronic control units (ECUs) are isolated, non-networked
  - Dedicated cables connect sensors and actors
  - Costly, heavy, error prone
  - Considerably limits system architectures, e.g. ECU placement

- Starting with the 90s, digital Bus systems are more widely applied
  - CAN-Bus networks
  - Split into individual busses by criticality level of communication
    - Safety relevant communication
    - Comfort functions
  - Replace several specialized cables with one bus system
  - Also support debugging, firmware updates, and hardware in the loop testing

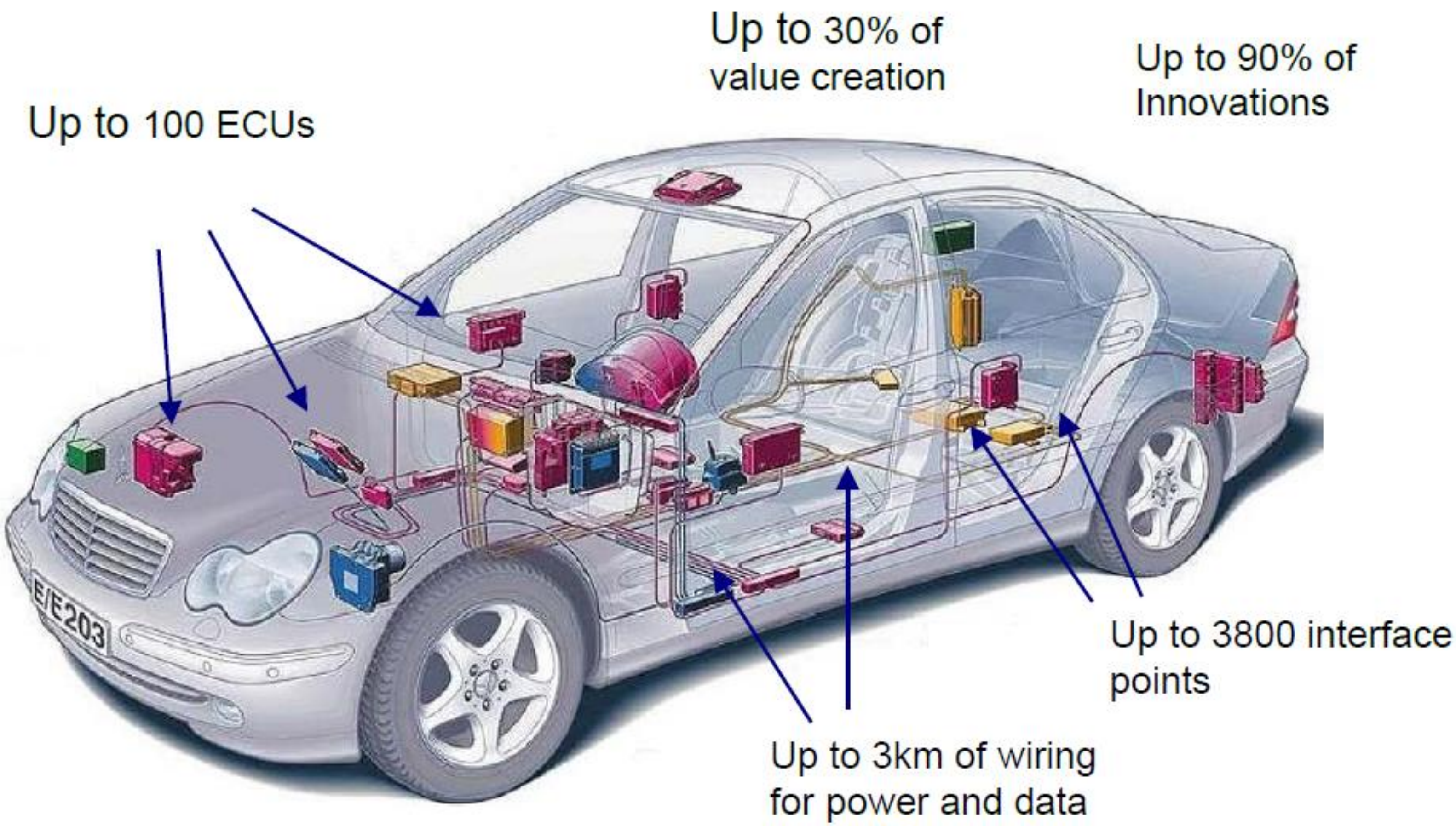
Introduction

Vehicular bus systems and networks today

- Rising demands on bus systems
  - Networked functionality requires more than one control unit
    - Gateways between bus systems become necessary
    - High Speed CAN, Flexray, MOST, Real-time Ethernet, ISOBUS
  - Demands to bus systems are increasing
    - Hardware virtualization for testing (CCP, XCP)
    - Real time constraints
    - Multimedia content
    - Safety relevant content
      - ABS/ESP
      - Radar/Camera pictures for pedestrian detection
      - X-By-Wire
      - Remote controlled functions

Introduction

Vehicular electronics and bus systems – growing importance



Introduction

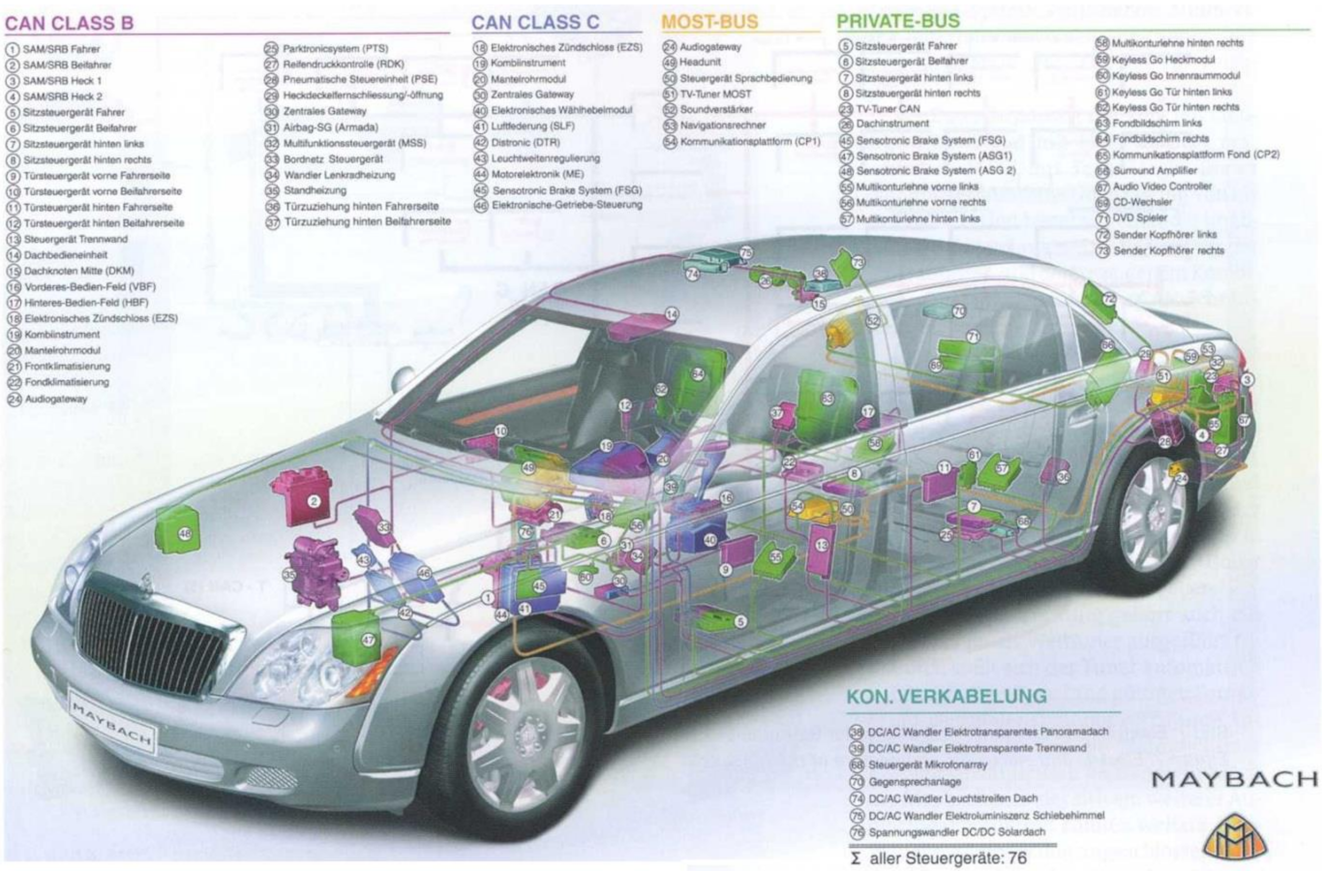
Vehicular architectures (today)

- Upper class vehicles carry 80 .. 100 networked Electronic Control Units (ECUs)
  - Traditionally: one function is processed by one ECU
    - One function (e.g. ABS) may consist of multiple tasks and runnables
    - Supports safety qualification of functions

Introduction

Vehicular architectures (today)

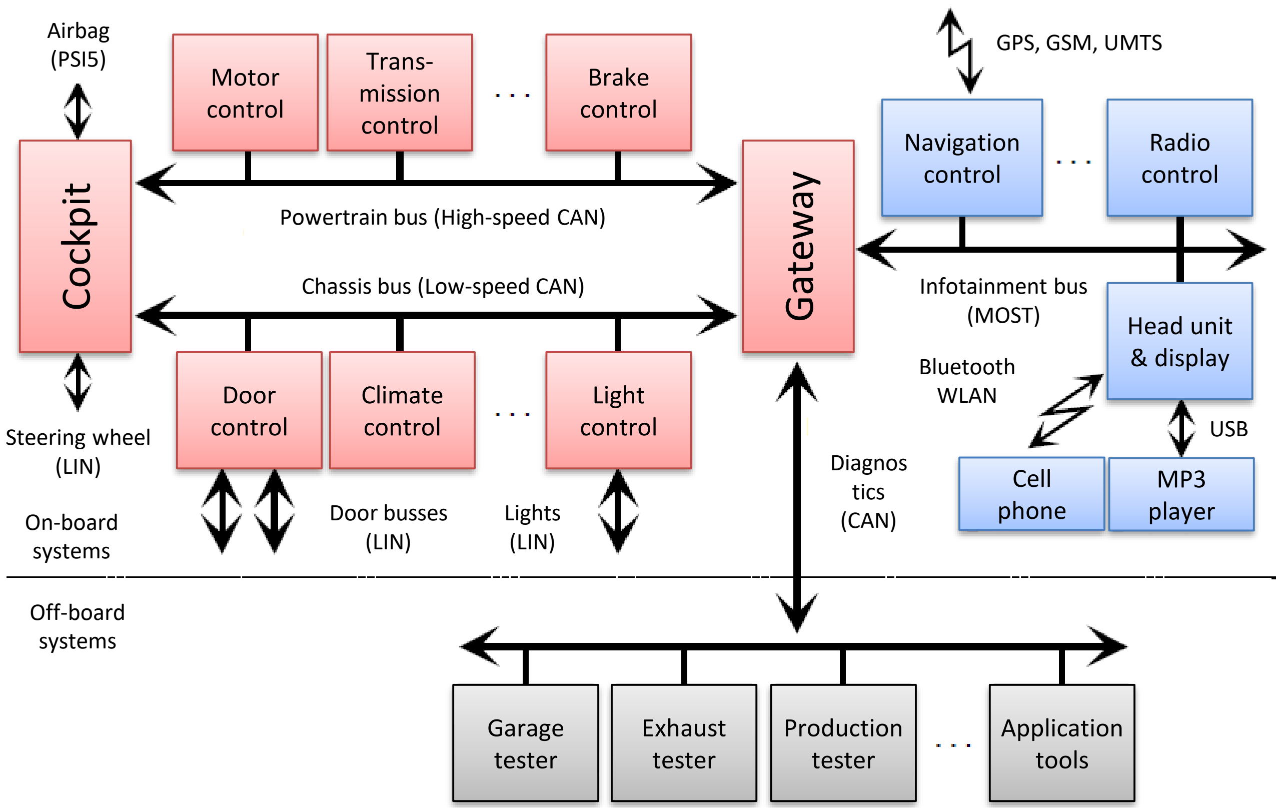
- Example for a current vehicular architecture



Introduction

Vehicular architectures (today)

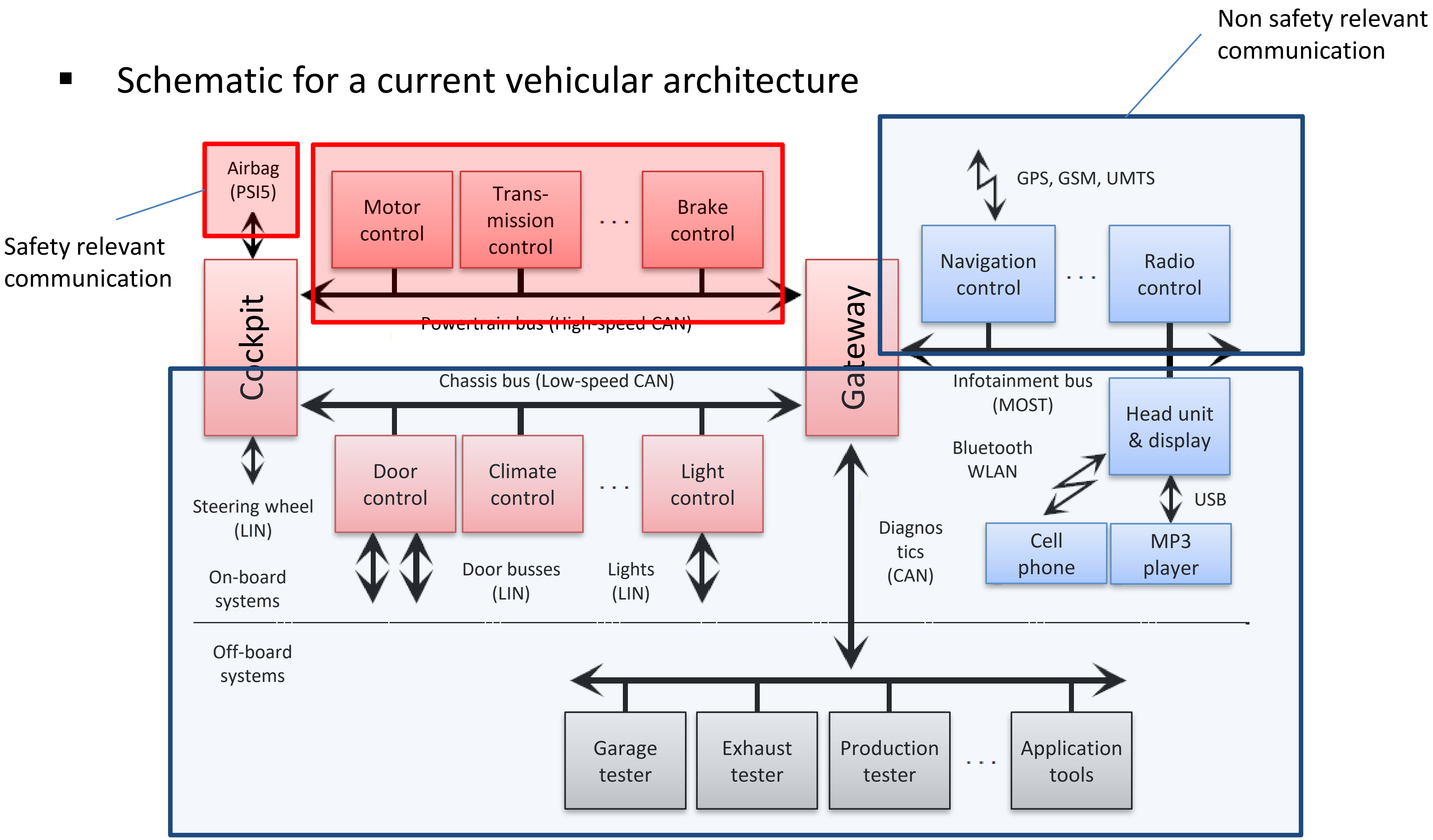
- Schematic for a current vehicular architecture



Introduction

Vehicular architectures (today)

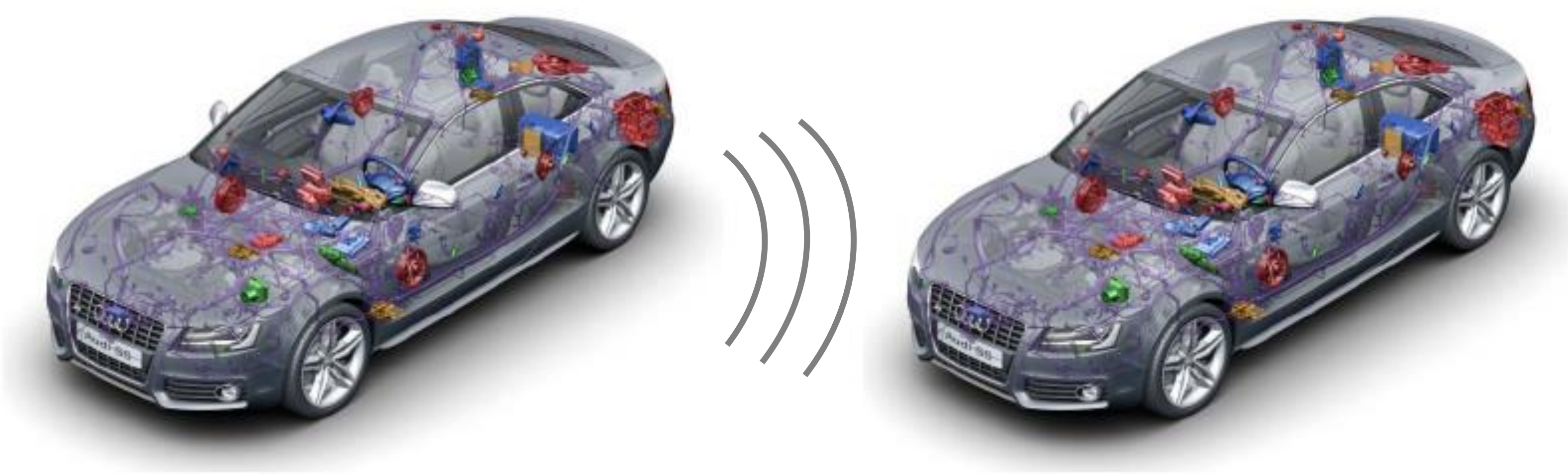
- Schematic for a current vehicular architecture



Introduction

Vehicular architectures (future)

- Trends
  - Distribution of functions among ECUs
  - Consolidation of different functions on the same ECU
    - Current strategy: consolidate functions by used actuators
    - Requires bus systems that enable tight coupling of distributed functions
  - Open Systems and wireless interfaces



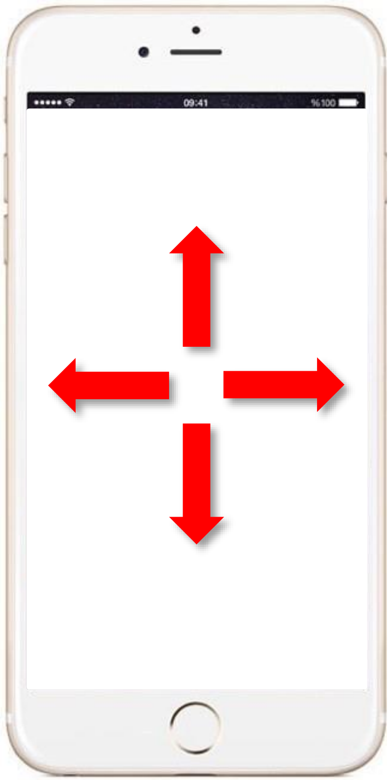
Introduction

Next generation bus systems

- Modern assistance systems are getting more and more networked
  - Bus systems are imperative for the realization of these functions
  - Bus systems are also imperative for system safety (and security!)
- Lets have a look on some examples
  - Early brakes: Hydraulic, was not dependent on bus systems
  - ABS: Depends on bus system, but does no any harm if bus system fails
  - Brake-By-Wire: Brake failure when bus communication fails…?
  - Remote controlled Brake By Wire: Additional safety and security concerns
- Future applications are impossible without modern bus systems
  - Most of them will require wireless communication as well

Introduction

Next generation bus system applications – example



Introduction

Next generation bus system applications – examples

- Open communication networks (Car-to-X communication)
  - Car to infrastructure communication
  - Car to car communication

- Wireless links become more important
  - Heterogeneous networks
- Todays challenges
  - Data integrity, timeliness
- Additional challenges
  - Fault detection
  - Self configuration
  - Programming interfaces
  - Security

Introduction

Discussion

- What is the main purpose of a communication system?

- What is quality of service?

- Which Quality of Service levels can you think of?

- Which factors limit QoS?

Introduction

Bus systems – Relevant components

- ISO/OSI Layered architecture – brief introduction
  - Standardizes internal functions and structure of communication protocols
    - Supports with managing the complexity of bus systems and protocols
  - Helps us to understand relevant (logical) components of bus systems and their interfaces

- Rationale: Structuring into layers
  - Each layer specifies one common functionality
  - A layer only communicates with its direct neighbours
  - Structures communication systems and enables re-use of functionalities
  - For example:
    - Physical encoding decoding
    - Medium access control
    - Management of logical connections
    - Application level communication (e.g. XCP)

Introduction

Communication System Architectures – Protocol stacks

- Implementation
  - Protocols do not need to use all layers
    - Communication protocols specify one or multiple layers
    - Depending on implemented functionality
  - In real protocols, we usually do not see a sharp 1:1 layer matching

Introduction

Communication protocol stacks

Application layer (Virtual Application Services)

Presentation layer (Application ⇔ Network formats)

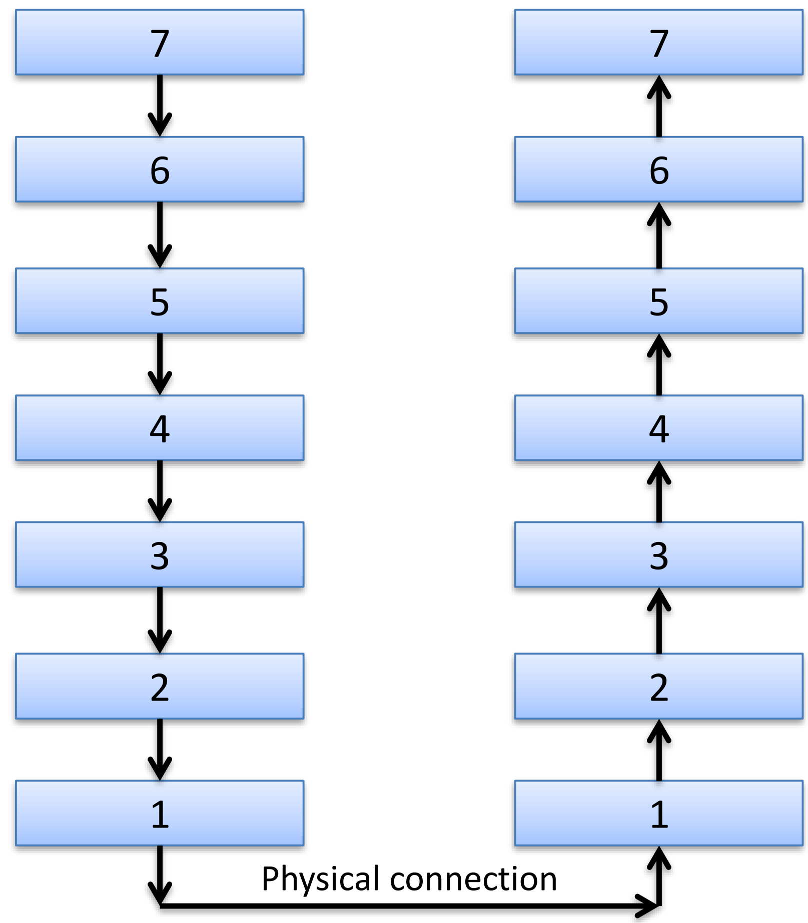
Session layer (Logical communication sessions)

Transport layer (Reliable end-to-end communication)

Network layer (Nodes of the same network)

Data link layer (Directly connected nodes)

Physical layer (Electrical/physical specification)



Introduction

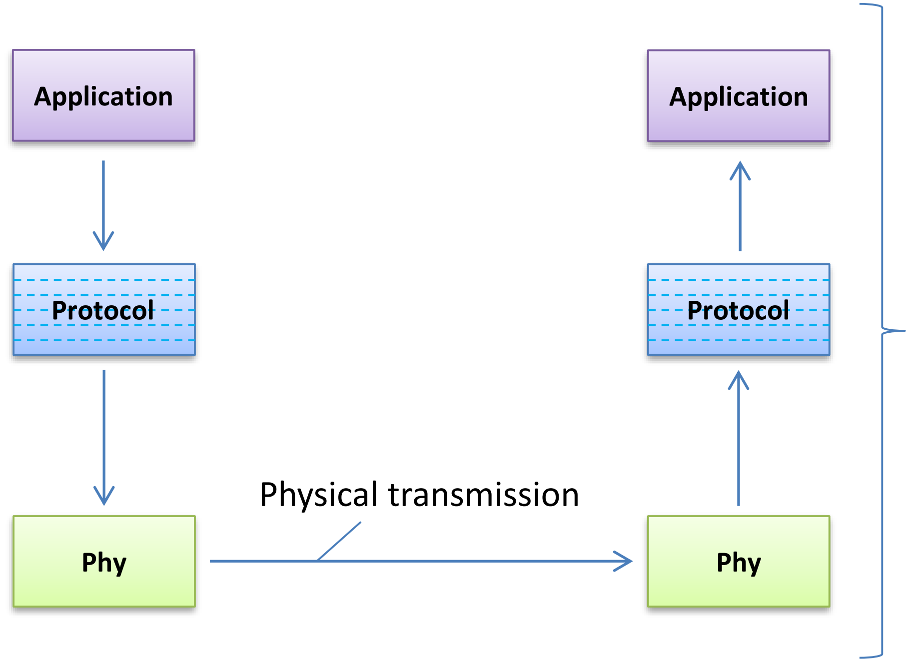
Bus systems – Relevant components

- What are we are going to cover in this lecture?
  - Things you need to know for analyzing, selecting, and applying bus systems

Application interface

Application level protocols
- CANOpen
- ISOBUS
- CCP/XCP

Bus level protocols
- CAN, Flexray
- Understanding
- Analysis
- Prediction



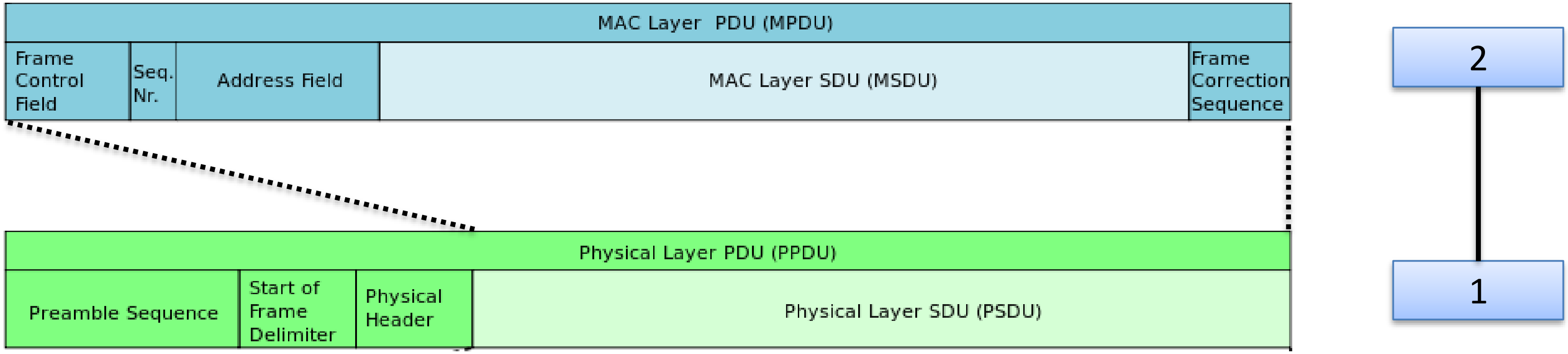
Domains
- Automotive
- Commercial vehicles
- Avionics
- Automation

Introduction

Communication protocol stacks – framing principle

- Framing approach for Protocol Data Units (PDUs)
  - When transmitting, lower level layers add frames to PDUs from upper layers
  - When receiving, layers remove their frame before transmitting PDU up
  - PDUs from other layers are considered payload and not evaluated further

- This approach enables re-use of protocol layers for different protocols



Introduction

Bus systems – non functional requirements

- Predictability
  - Ability to predict bus system performance
  - Message transmission times, message jitter, available bit rate
- Scalability
  - Ability to adapt to changing communication requirements
  - Ability to include additional devices or services
- Reliability
  - Ability to guarantee correct transmission, reception, and data integrity
  - Ability to detect transmission errors
- Robustness / Availability
  - Ability to provide potentially degraded functionality even in case of errors

Introduction

Bus systems – non functional requirements

- Robustness / Availability
  - Ability to provide potentially degraded functionality even in case of errors
- Privacy
  - Ability to prevent unwanted reading of data
  - Ability to detect/prevent unauthorized data modification
  - Ability to detect/prevent unauthorized data transmission
  - Ability to detect/prevent spoofing of data / faking transmitter IDs

Introduction

Bus systems are erelevant to most embedded systems

- Embedded Systems are often safety critical and need to communicate
  - We know about non functional properties that are relevant to bus systems
  - What happens when a bus system cannot fulfill these properties anymore?
    - When could a bus system fail or degrade?
    - Why could something like this happen?
    - How could one potentially work around this or reduce the impact?

  - Communication errors cannot be fully prevented, but must be manageable
    - Either by machine, or by operator
    - Not all of these errors are manageable at bus system level
      - Discussion: Can you give an Example?

  - Identification and management of potential communication errors in safety relevant systems is part of safety concept
    - Requires system level knowledge

Introduction

Safety relevant bus systems

- Discussion: Why is Safety never a property of an individual bus system?
  - Safety is a system property
    - Requires consideration of application scenario, environment, user behavior, technical domain, functional behavior, and bus systems
  - Bus system properties affect safety and safety concepts for safety relevant systems
    - Definition of countermeasures to address bus system failures
    - Evidences (guarantees) provided by bus systems
    - Requires the understanding of bus systems, their concepts, physics, and protocols

Introduction

Safety relevant bus systems

- Safety
  - The condition of being protected against consequences of failure, damage, error, accidents, harm or any other event which could be considered non-desirable.
  - Control of recognized hazards to achieve an acceptable level of risk.
  - Being protected from the event or from exposure to something that causes health or economical losses.

- Safety concept
  - Risk prevention and management strategy
  - Based on identification and analysis of harzards, and on application of remedial controls
  - Includes fail-safe and fail-operational measures

Introduction

Safety relevant bus systems – Failures

- Not fulfilling the previously mentioned criteria could lead to system failure
- Failure
  - Undesired behavior of a given device under defined conditions
- Failure mode
  - Describes the way a failure occurs
  - Specific manner by which a failure occurs in the system
- Hazard
  - Individual threat that *could* cause a failure mode

Introduction

Safety relevant bus systems – Failures

- Examples
  - Failure: Brake does not work anymore
  - Failure mode: Communication failure due to broken copper wire
  - Hazard: Braking of a copper wire

  - Failure: Brake does not operate reliably
  - Failure mode: Communication is delayed due to concurrent bus accesses
  - Hazard: Other nodes blocking the bus with low priority data

- Can there be multiple failure modes for the same failure?

Introduction

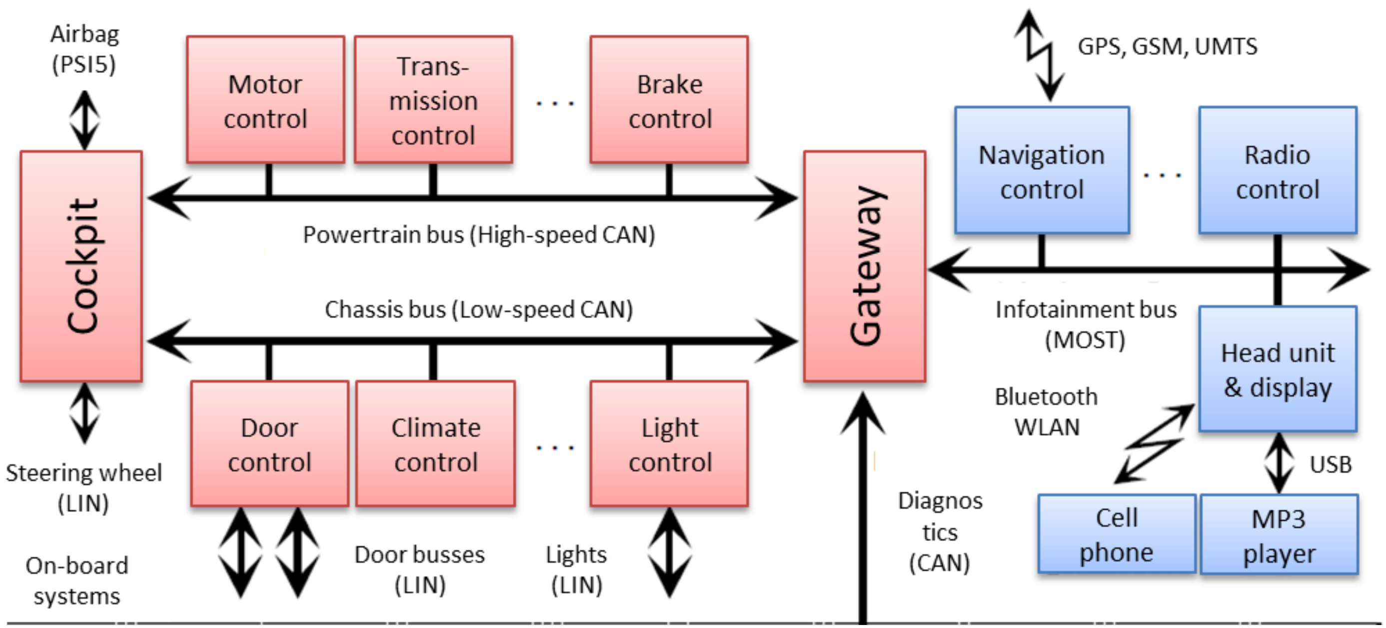
Safety relevant bus systems – Properties

- Ideal Bus systems from a safety perspective are:
  - Reliable
    - Transmission errors should not occur (but cannot be avoided)
    - Transmission errors should be detected (which methods can you think of?)
    - Transmission errors should be correctable in high risk areas
    - Acceptable error rate depends on application area
  - Predictable
    - Maximum bounds for communication delay and jitter must be guaranteed
  - Scalable
    - Quality of Service must be independent of the number of communicating nodes
    - Especially for wireless systems
  - Robust
    - Must not malfunction or fail completely in case of isolated errors

Introduction

Safety relevant bus systems

- Example: Prototyping of an automotive remote control unit
- How do we need to extend the system
- Which hazards, failure modes and failures could you identify?
- Which countermeasures would you propose?



Introduction

Safety relevant communication systems - Discussion

- Can you always guarantee that a failure does not occur?
  - System designs must handle possible failure modes in a satisfactory manner
  - New generations of bus systems introduce additional failures and failure modes
  - Systems evolve and system architectures are not always prepared for new bus systems
    - Could you think of an example?

- Failures may occur on many levels
  - Good understanding of bus systems and the responsibilities of their components is imperative
  - Sound system architectures ensure error and threat isolation