EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

FACULTY OF
SCIENCE
Communication Networks

Softwarization of Automotive E/E Architectures
A Software-Defined Networking Approach

M. Häberle, F. Heimgärtner, H. Löhr, N. Nayak, D. Grewe, S. Schildt, M. Menth

http://kn.inf.uni-tuebingen.de

Outline

- Motivation
- Evolution of E/E-Architectures
- Use Case: Trailer Networks
- Architecture
  - Overview
  - Data Plane
  - Management
- Operations
  - TSN Configuration
  - Failover
- Security

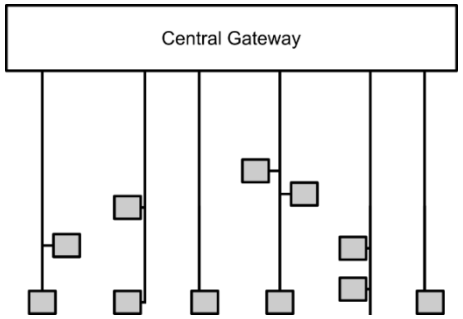
Motivation

- In-vehicle networks today
  - Low bandwidth technologies
  - Static configuration, determined during manufacturing
- Future
  - More bandwidth demand
    - Autonomous driving
  - Configuration changes after purchase
    - Plug-and-play add-on components
    - Updates or downloadable features
- Reconfigurable networks required
  - Apply SDN principles

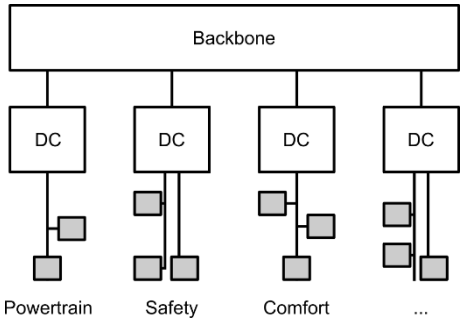
Evolution of E/E-Architectures

- Distributed ECUs connected to single CAN bus
- Multiple CAN buses connected to central gateway
  - Additional application-specific buses (LIN, MOST, FlexRay)
- Consolidation of functionality into more powerful devices
  - Vehicle computers with virtualization
  - Domain model
    - ECUs separated into Domains (safety, comfort, infotainment,…)
    - One or more buses per domain connected to domain controller
    - Domain controllers connected by backbone network
    - Problem: wiring effort
  - Zone model
    - Zone controllers per location (front left/right, rear left/right,…)
    - ECUs connected to local zone controllers
    - Zone controllers interconnected by backbone network (mesh)
- Automotive Ethernet
- Time Sensitive Networking

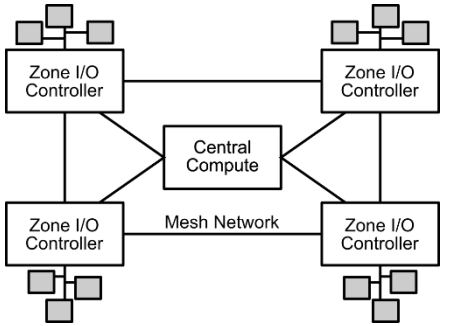
Topology with a central gateway



Domain model



Zone model

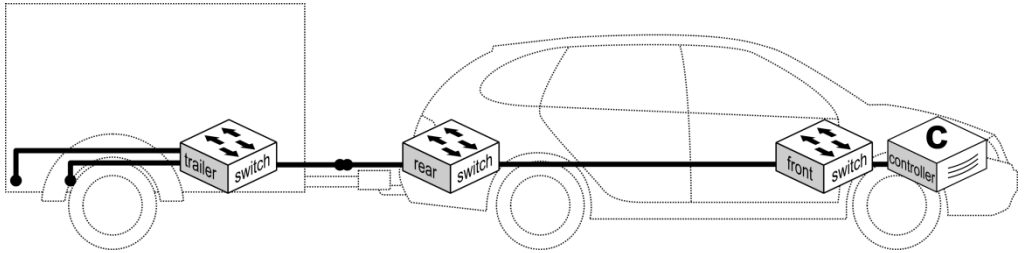


Use Case: Trailer Networks

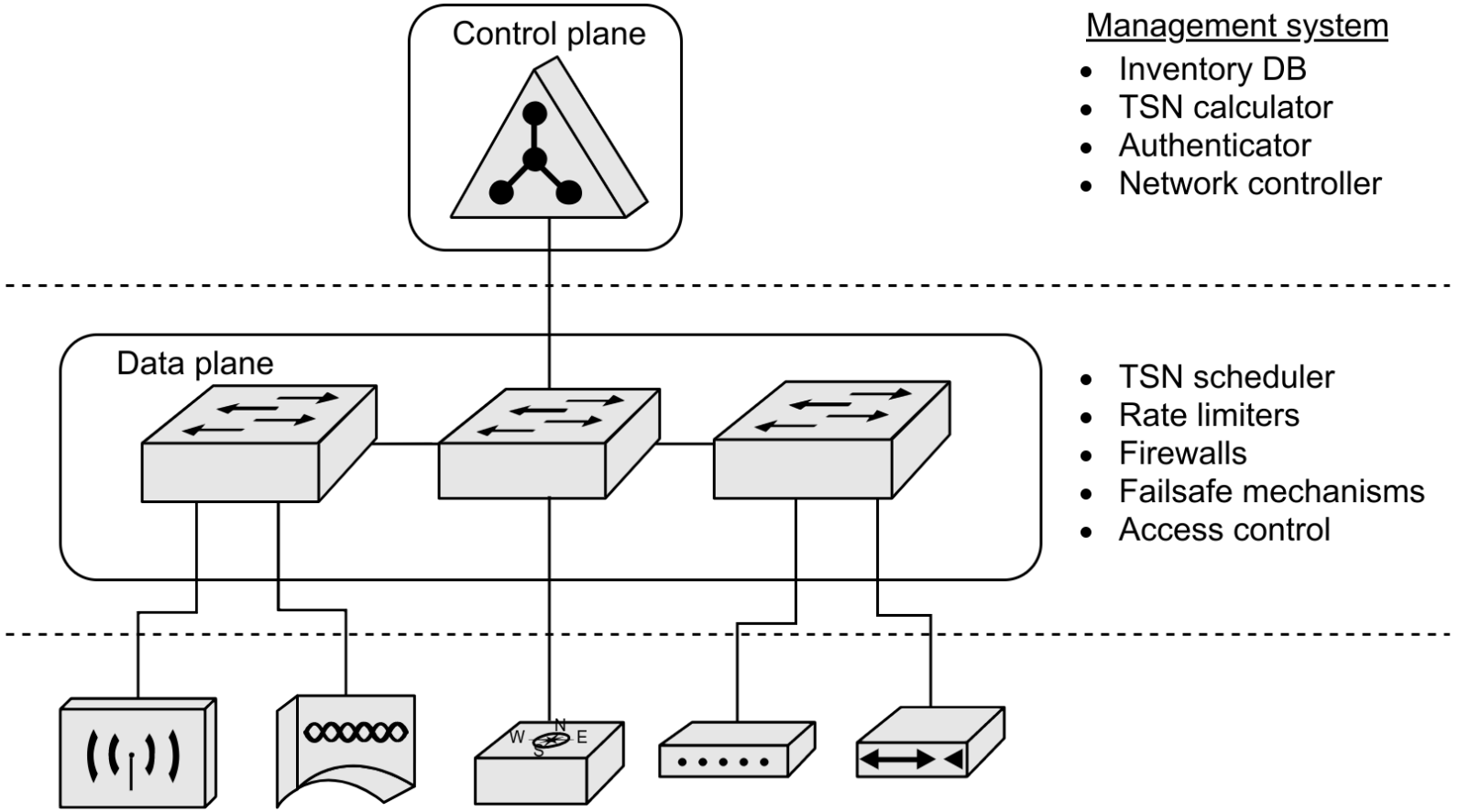
- Trailer connection today
  - Electrical connection (5-22 pins)
  - Fixed function set (tail lamps, turn signals, electric brakes)

- Future
  - Switches in car and trailer
  - Ethernet connection

- Benefits from reconfigurable networks
  - Connection of networked components in trailer to vehicle
    - Cameras
    - Sensors (e.g., park distance control)
    - Actuators (e.g., electric brakes with TSN)
  - Sharing of uplink
    - Wi-Fi AP in caravans/camping trailers
    - Monitoring freight trailers

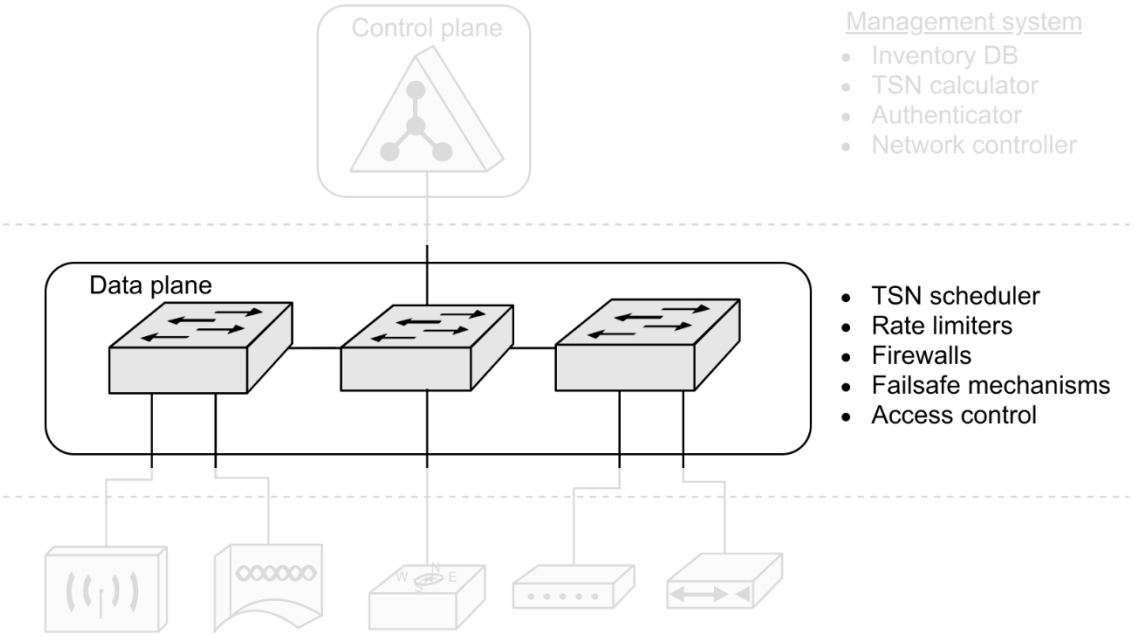


Automotive SDN Architecture



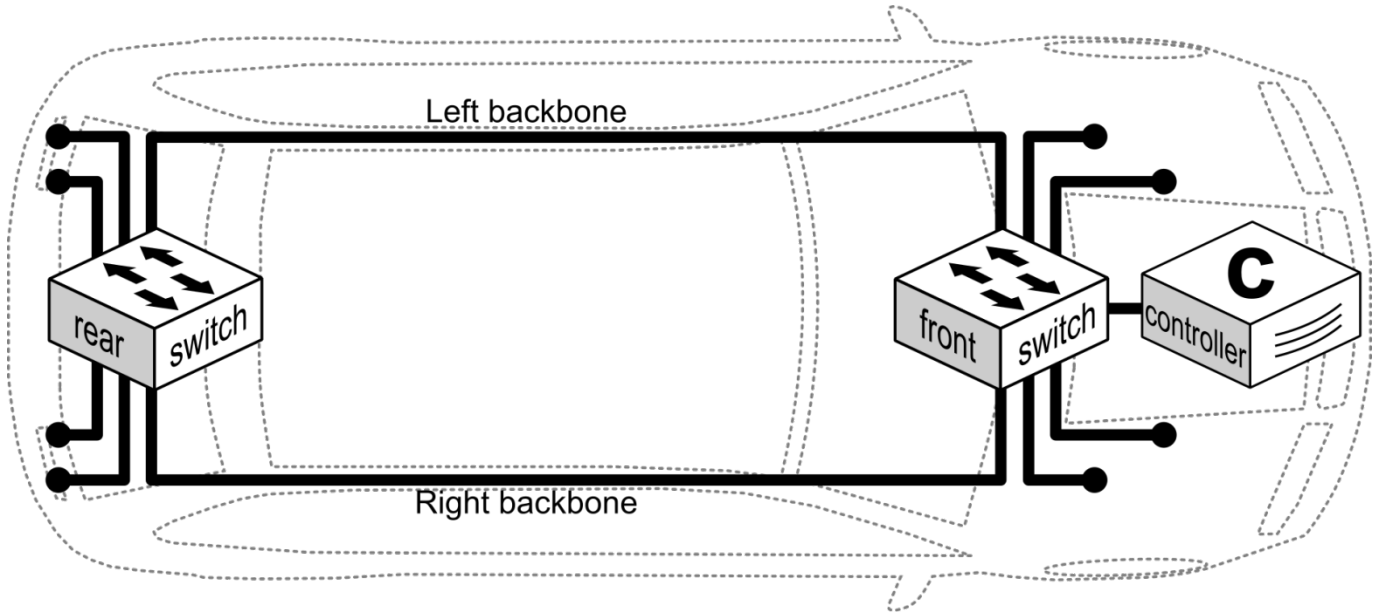
Data Plane

- Functionality
  - Interconnect components and applications
  - Connect components and applications to management system



- Traffic classes
  - Hard real-time
    - Safety-critical components
    - Fixed deadlines
  - Soft real-time
    - Less critical systems
    - Degraded operation possible with missed deadlines
  - Configuration
    - Management
    - Device discovery
  - Best effort
    - Infotainment
    - All other traffic

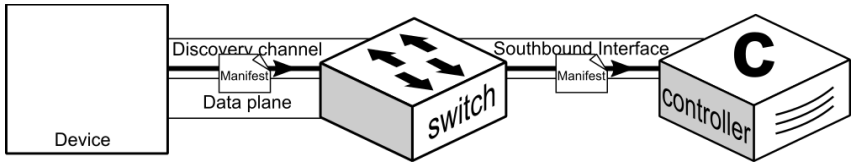
Topology



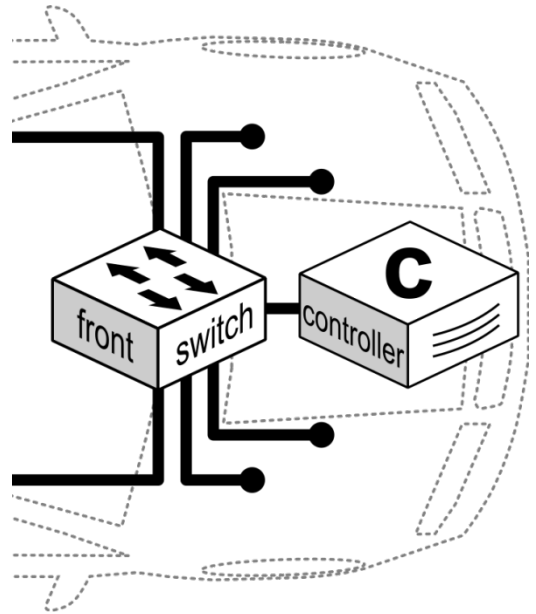
- Two switches (front and rear switch)
- Two backbone links between front and rear
  - Link aggregation during normal operation
  - 1+1 protection for selected critical flows
  - Rescheduling traffic to the operational link in case of link failure

Management

- Data plane configured by network controller
- Controller directly connected to one of the switches
- In-band signaling
  - Reduced wiring effort
  - Extensibility (trailer use case)
- Discovery mechanism
  - Automatic discovery of new devices and newly installed applications
  - Access to discovery channel only at first, other traffic blocked
  - New Device sends signed manifest, triggers reconfiguration
    - Identification
    - Connectivity requirements



- Northbound interface
  - Used to trigger reconfigurations
  - Access restricted by ACLs and permission levels



Operations: TSN Configuration

- Safety-critical components require real-time communication

- Updates of Time Sensitive Networking (TSN) configuration
  - Allocation of bandwidth
  - Re-calculation of schedules
  - Path selection for 1+1 protection

- Hybrid scheduling
  - First: In-car controller calculates initial schedule
    - Starts immediately when necessary
    - Not enough computing resources to calculate optimal schedule
    - Non-optimal, with approximations
    - Guarantees for safety-critical systems only
  - Second: Cloud service is triggered for schedule calculation
    - Starts as soon as Internet connection is available
    - Enough computing resources to compute optimal schedule
    - Re-use cached schedule for same constellation
    - Compute optimal schedule if no cached schedule available

Operations: Failover

- Single backbone link failure
  - Traffic is rerouted trough remaining backbone link
  - Pre-calculated outage schedule for TSN flows

- Controller failure
  - No reconfiguration possible anymore
  - Backup flows and schedules pre-computed for critical systems
  - Switches apply backup configuration if connection to controller lost

- Switch failure or double backbone link failure
  - Components enter fail-safe state
  - Backup systems to ensure safe stop of vehicle

Security

- Devices and Applications
  - New devices can only access network for discovery
  - Manifest signature by trusted manufacturer required
  - Device sends app manifest to controller via northbound API
  - Central CA store contains CA certificates

- Network security
  - Specific flows between devices and applications
    - No wildcard flows
    - Attacker can’t attack devices he can’t reach
  - Firewall for outside connections
    - Filtering of uplink, V2X, Bluetooth, Wi-Fi
  - MACsec or AUTOSAR SecOc for integrity protection
  - Access restrictions for controller interfaces

Conclusion

- Legacy automotive networks
  - Low bandwidth
  - Static configuration
- New applications and use cases
  - Demand for higher bandwidth
  - Need for more flexibility
- Technology for future automotive networks
  - Automotive Ethernet
  - Time-Sensitive Networking
- SDN concepts for automotive Ethernets
  - Configuration and management
  - Path selection
  - TSN schedules
  - Access control

Contact

Marco Häberle
marco.haeberle@uni-tuebingen.de
University of Tuebingen, Dept. of Computer Science
Chair of Communication Networks
Sand 13, 72076 Tuebingen, Germany
http://kn.inf.uni-tuebingen.de/