EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

MATHEMATISCH-
NATURWISSENSCHAFTLICHE FAKULTÄT

Kommunikationsnetze

An SDN Architecture for Automotive Ethernets

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 Cases
  - Trailer Networks
  - Driver Assistance Systems
- Architecture
  - Overview
  - Data Plane
  - Management
- Operations
  - TSN Configuration
  - Discovery
  - Failover
- Security

Motivation

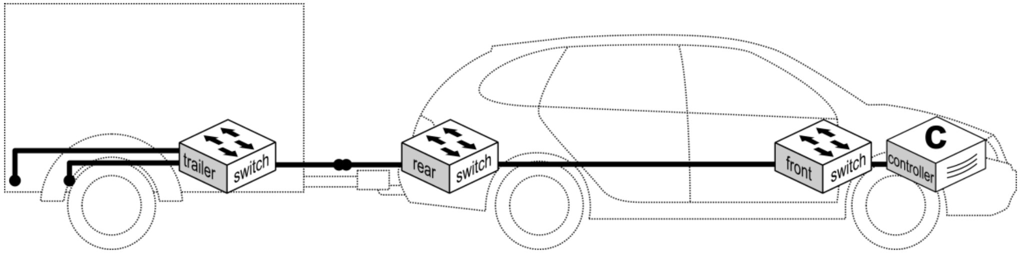
- In-vehicle networks today
  - Low bandwidth technologies
  - Static configuration, determined during manufacturing
- Future
  - More bandwidth demand
  - Configuration changes after purchase
    - Plug-and-play add-on components
    - Downloadable features
- Reconfigurable networks required

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
  - 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

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 (e.g., Wi-Fi for caravans/camping trailers)

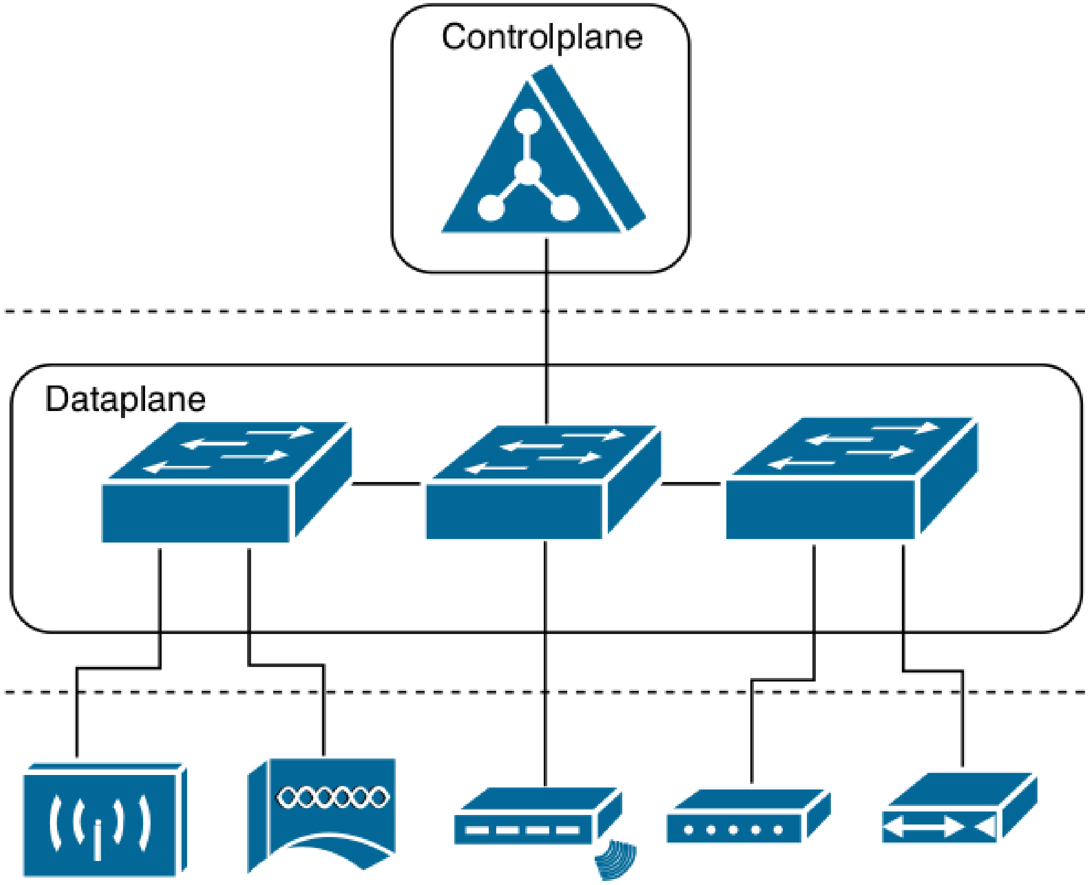
Use Case: Driver-Assistance Systems

- Downloadable driver-assistance systems or OTA updates

- Benefits from reconfigurable networks
  - Change of data sources (sensors, etc.)
  - Reconfiguration of real-time streams

- Example: Update of collision avoidance system
  - Initial feature set
    - Check forward traffic only
  - Update
    - Check backward traffic while reversing
  - Needs access to reversing camera or PDC sensors
  - Re-configuration of network required

Automotive SDN Architecture



- Inventory DB
- Permissions DB
- TSN Calculator
- Authenticator
- Network Controller

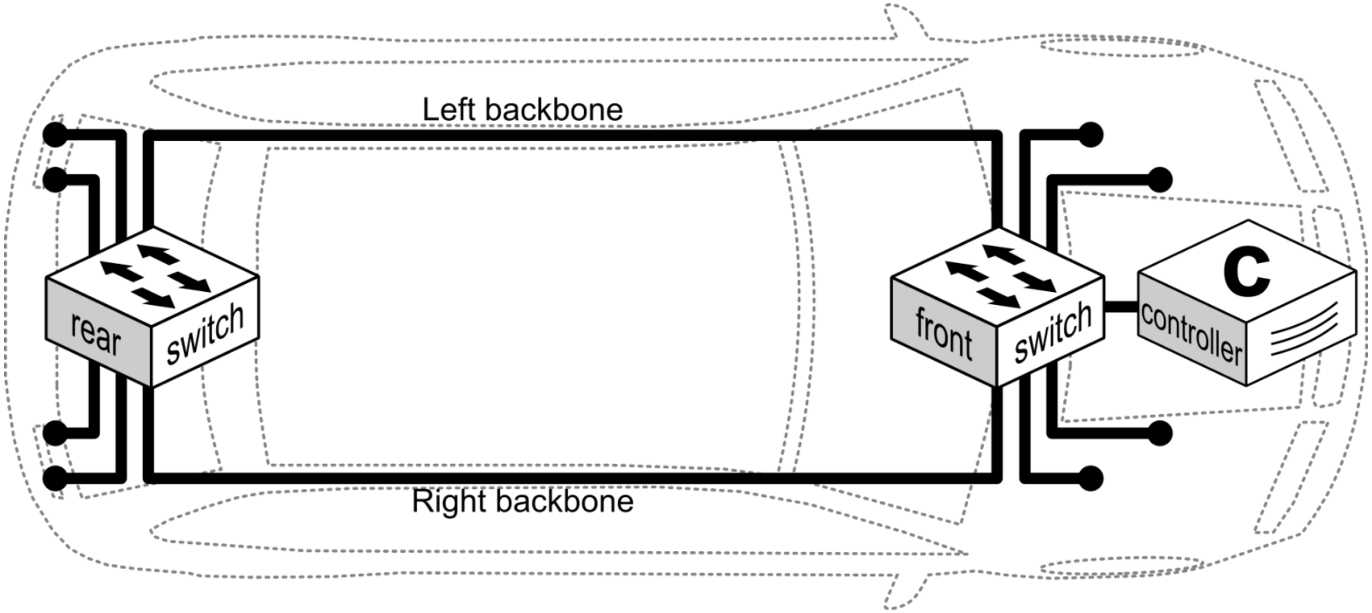
- TSN Scheduler
- Firewall
- Failsafe Mechanisms
- Access Control

Data Plane

- Components
  - Scheduler
  - Rate limiter
  - Firewall
  - Fail-safe mechanisms
  - Redundant links
  - Access control
- 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
    - Discovery
  - Best effort
    - Infotainment
    - All other traffic

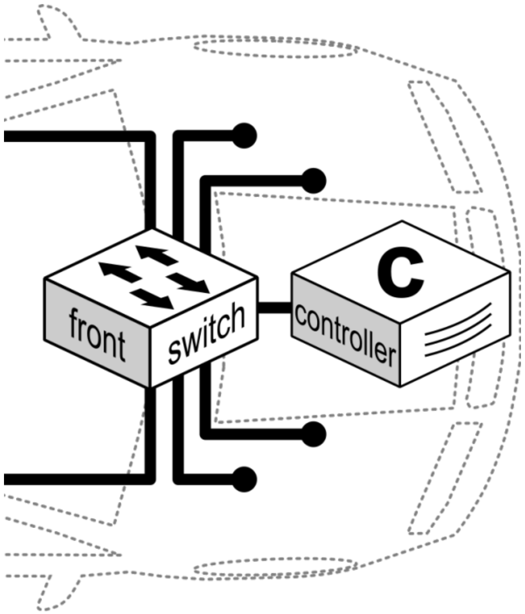
Topology



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

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)
- 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
  - In-car controller calculates initial schedule
    - Guarantees for safety-critical systems
    - Non-optimal, with approximations
  - Cloud service is triggered for schedule calculation
    - Re-use cached schedule for same constellation
    - Compute optimal schedule if no cached schedule available

Operations: Discovery

- Discovery of devices based on signed manifest
  - Network ports of switches blocked initially, only discovery channel open
  - New device sends manifest via broadcast message on discovery channel
    - Contains information about device (identification, requirements to network, access to northbound API of controller required, …)
    - Signed by manufacturer of device
    - External store of CA certificates, local cache
  - Controller re-configures network, gives access to northbound API if requirements of device are not static (e.g. if apps can be installed)
- Application discovery similar
  - Difference: Manifest sent by Host device via northbound API

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 signed 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
  - 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
  - Higher bandwidth demand
  - More flexibility needed
- 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, MSc.

haeberle@informatik.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/