The Rise and Evolution of Automotive Gateways

Brian Carlson

Product Management - AMP Connectivity & Security

October 2018 | AMF-AUT-T3384

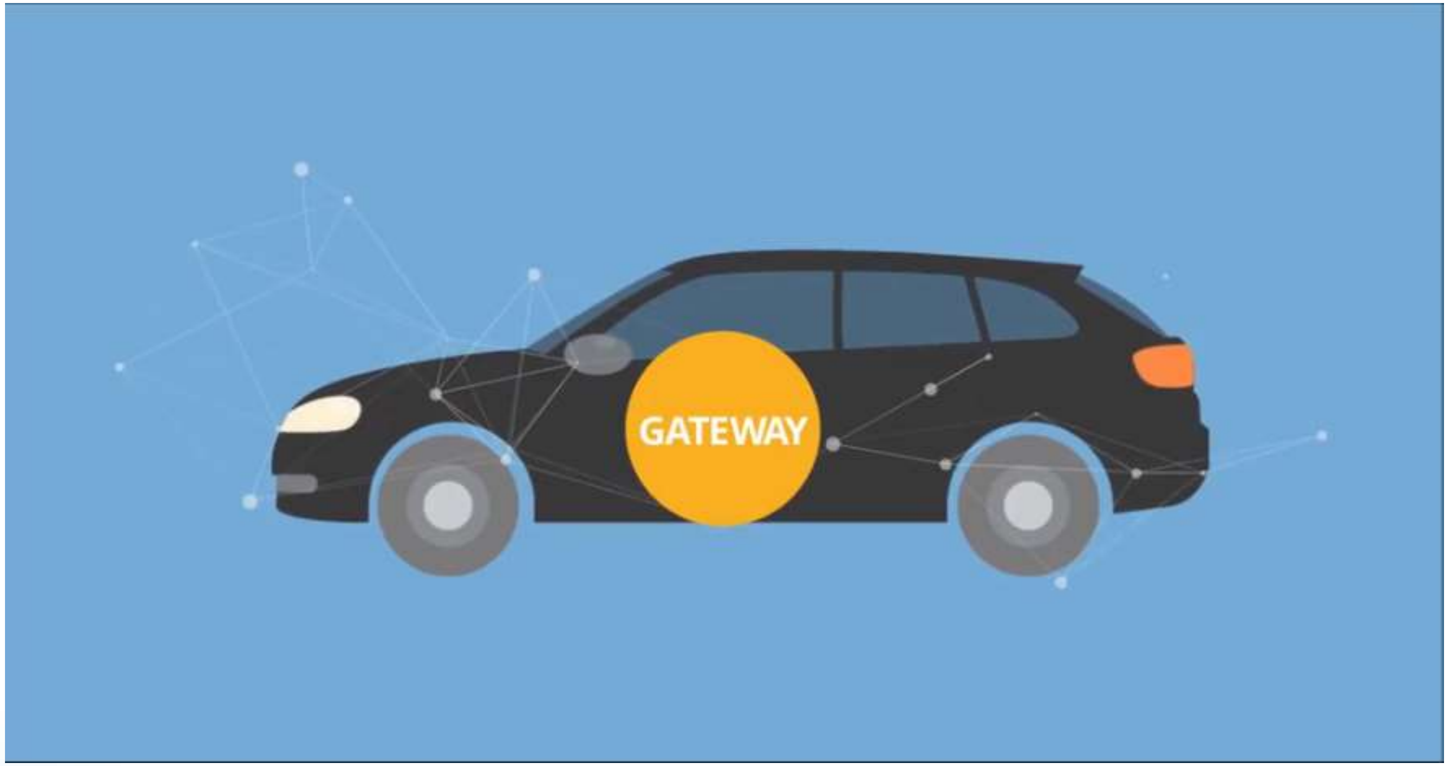
NXP | SECURE CONNECTIONS FOR A SMARTER WORLD

Company Public – NXP, the NXP logo, and NXP secure connections for a smarter world are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2018 NXP B.V.

Agenda

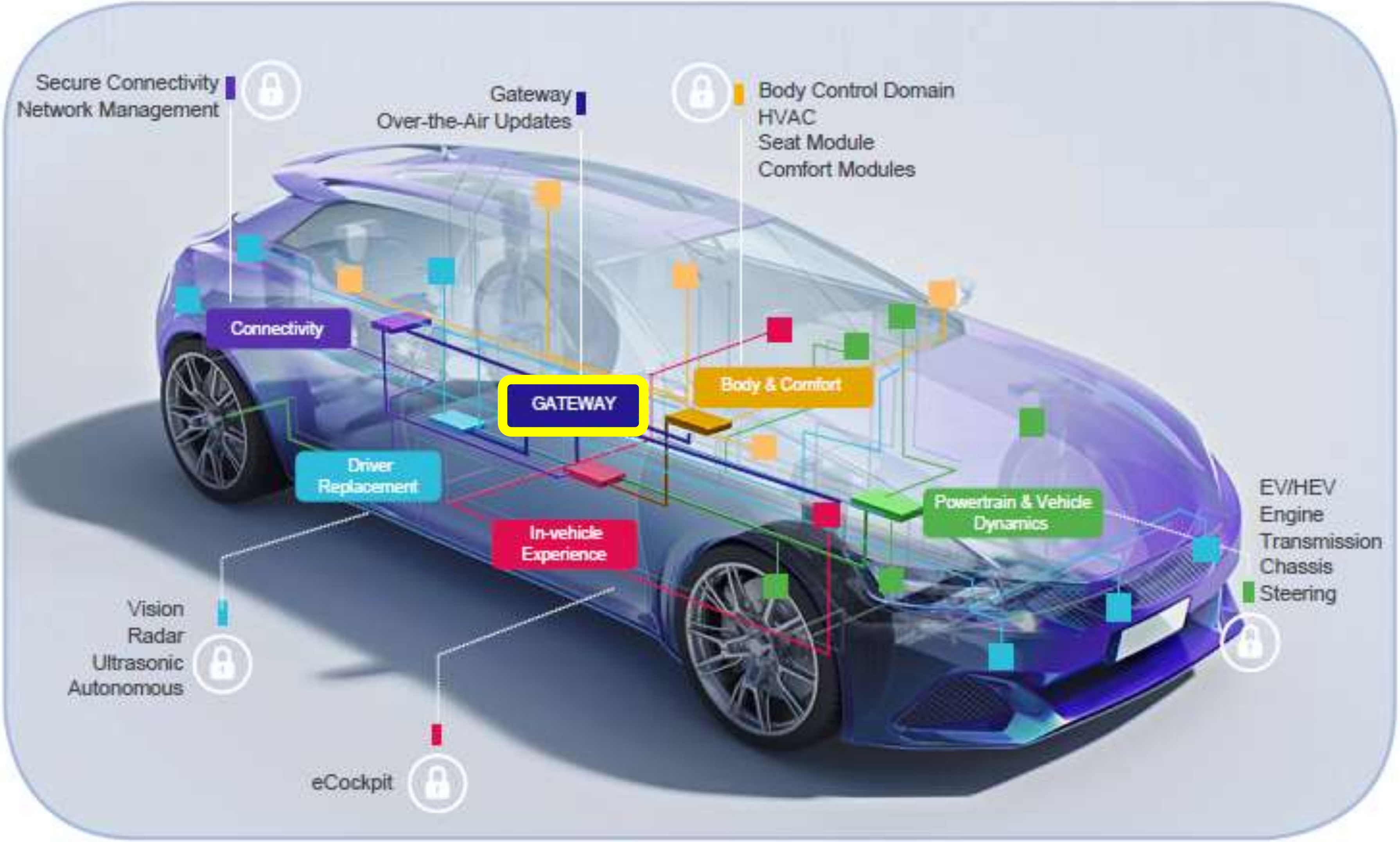
- **What is an Automotive Gateway?**
- **Gateway Evolution**
  - Overview, Market Trends, Architecture
- **NXP Gateway Reference Solutions**
- **Summary**
- **For More Information**

What is an Automotive Gateway?

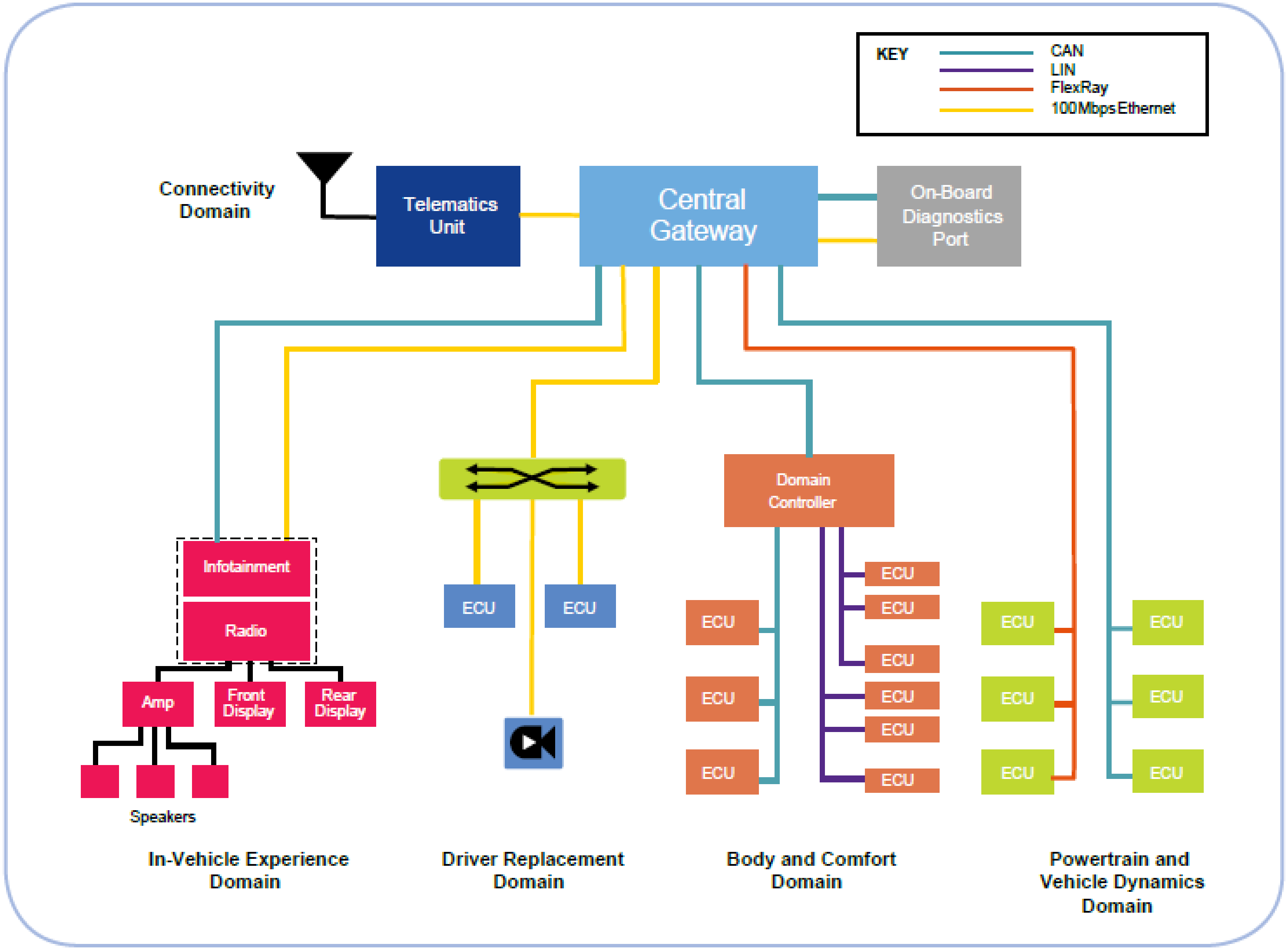


https://www.nxp.com/video/:AUTOMOTIVE-GATEWAY-VID

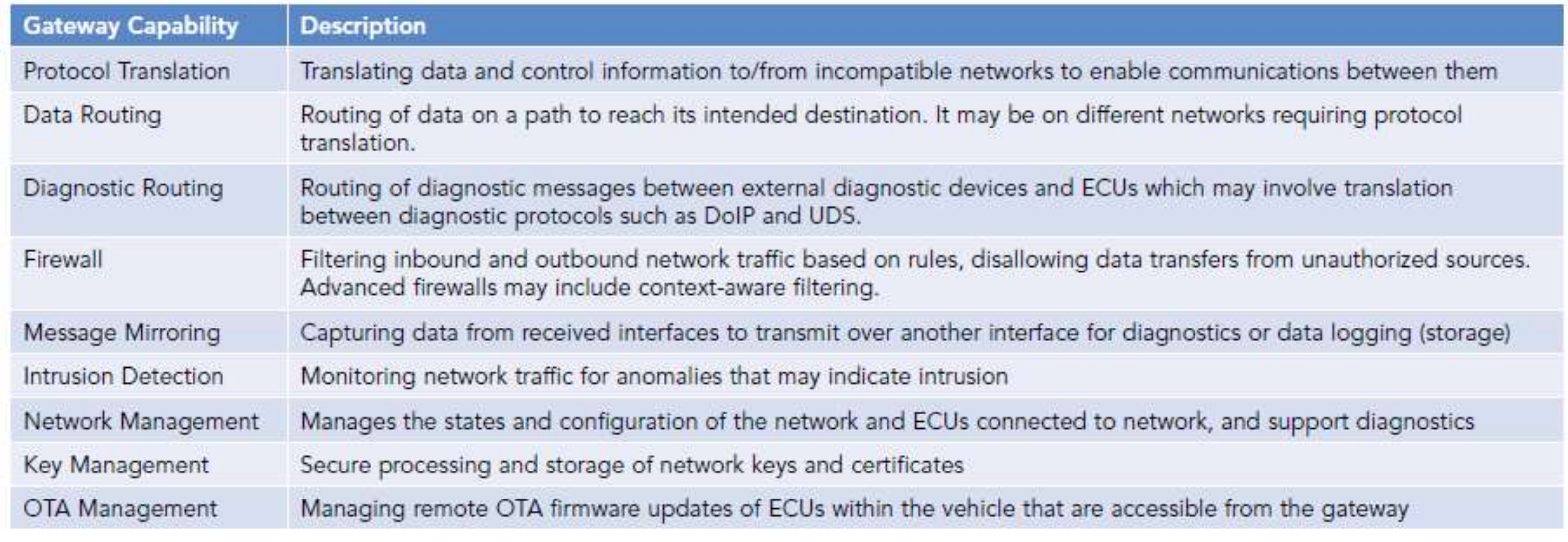
The Automotive Gateway is Central to the Vehicle



Automotive Gateway is Central for Vehicle Communications



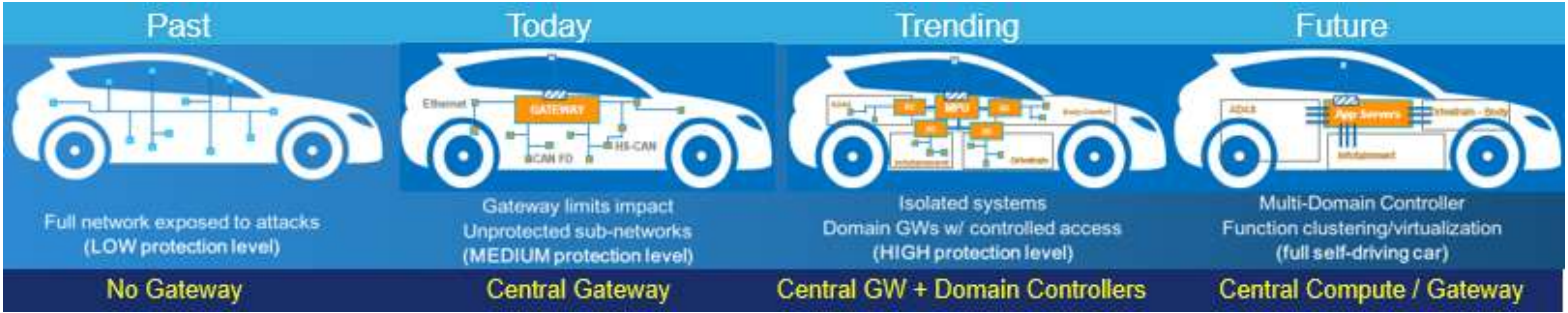
Key Gateway Functions



Gateway Capability	Description
Protocol Translation	Translating data and control information to/from incompatible networks to enable communications between them
Data Routing	Routing of data on a path to reach its intended destination. It may be on different networks requiring protocol translation.
Diagnostic Routing	Routing of diagnostic messages between external diagnostic devices and ECUs which may involve translation between diagnostic protocols such as DoIP and UDS.
Firewall	Filtering inbound and outbound network traffic based on rules, disallowing data transfers from unauthorized sources. Advanced firewalls may include context-aware filtering.
Message Mirroring	Capturing data from received interfaces to transmit over another interface for diagnostics or data logging (storage)
Intrusion Detection	Monitoring network traffic for anomalies that may indicate intrusion
Network Management	Manages the states and configuration of the network and ECUs connected to network, and support diagnostics
Key Management	Secure processing and storage of network keys and certificates
OTA Management	Managing remote OTA firmware updates of ECUs within the vehicle that are accessible from the gateway

Gateway Evolution – Overview

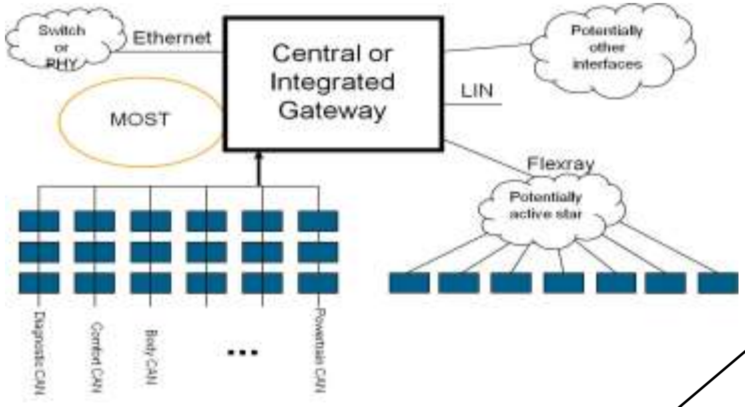
Gateway Rise and Evolution



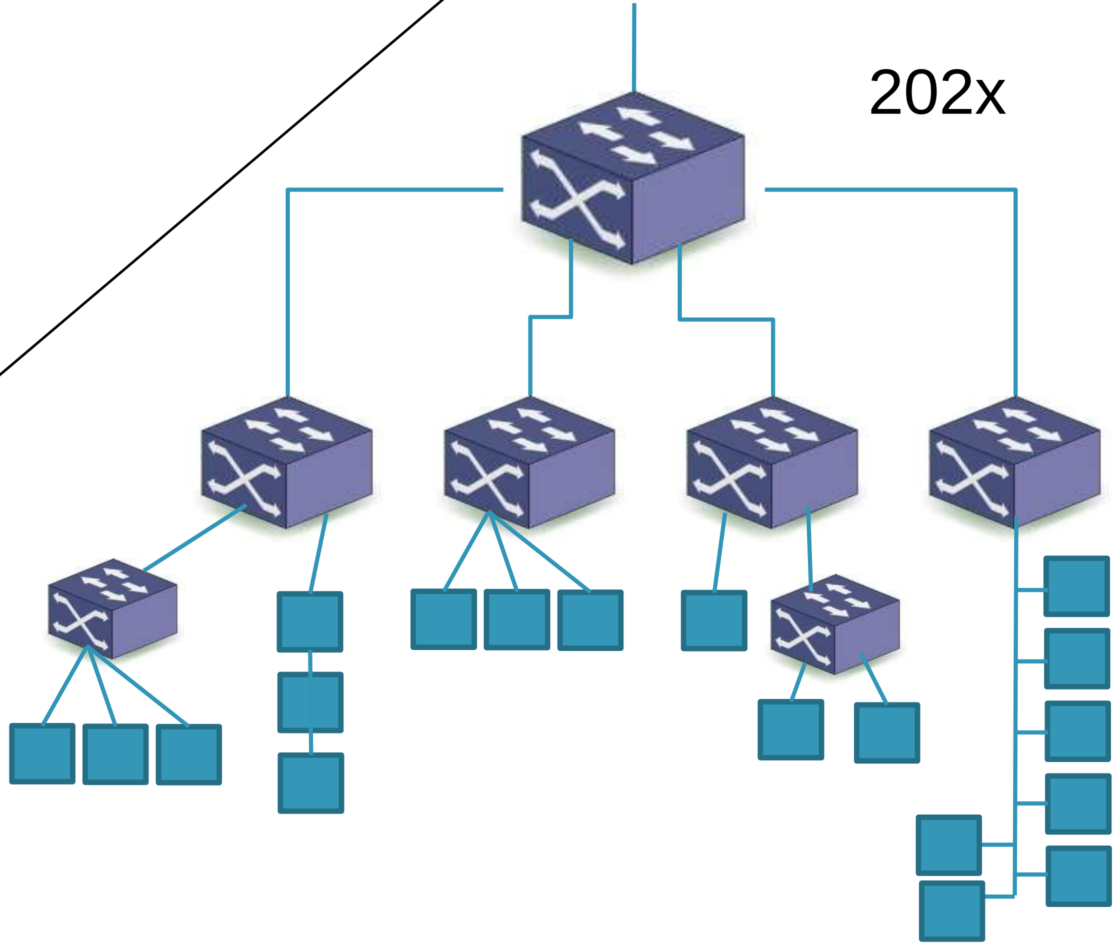
Past	Today	Trending	Future
Full network exposed to attacks (LOW protection level)	Gateway limits impact Unprotected sub-networks (MEDIUM protection level)	Isolated systems Domain GWs w/ controlled access (HIGH protection level)	Multi-Domain Controller Function clustering/virtualization (full self-driving car)
No Gateway	Central Gateway	Central GW + Domain Controllers	Central Compute / Gateway

• No or limited connectivity	Connectivity	• High-speed wireless interfaces
• No or limited security	Security	• High security, isolation, public key crypto, contextual firewall, intrusion detection
• Basic routing	Processing	• Advanced routing, vehicle OTA, analytics, ECU consolidation, services
• Limited bandwidth / scalability (kilobit / Megabit interfaces)	Networking	• High-bandwidth, scalable architectures (Gigabit interfaces)
• Up to ASIL B with fail safe	Functional Safety	• Up to ASIL D with fail operational

Evolution from Central Gateway to Distributed Architecture

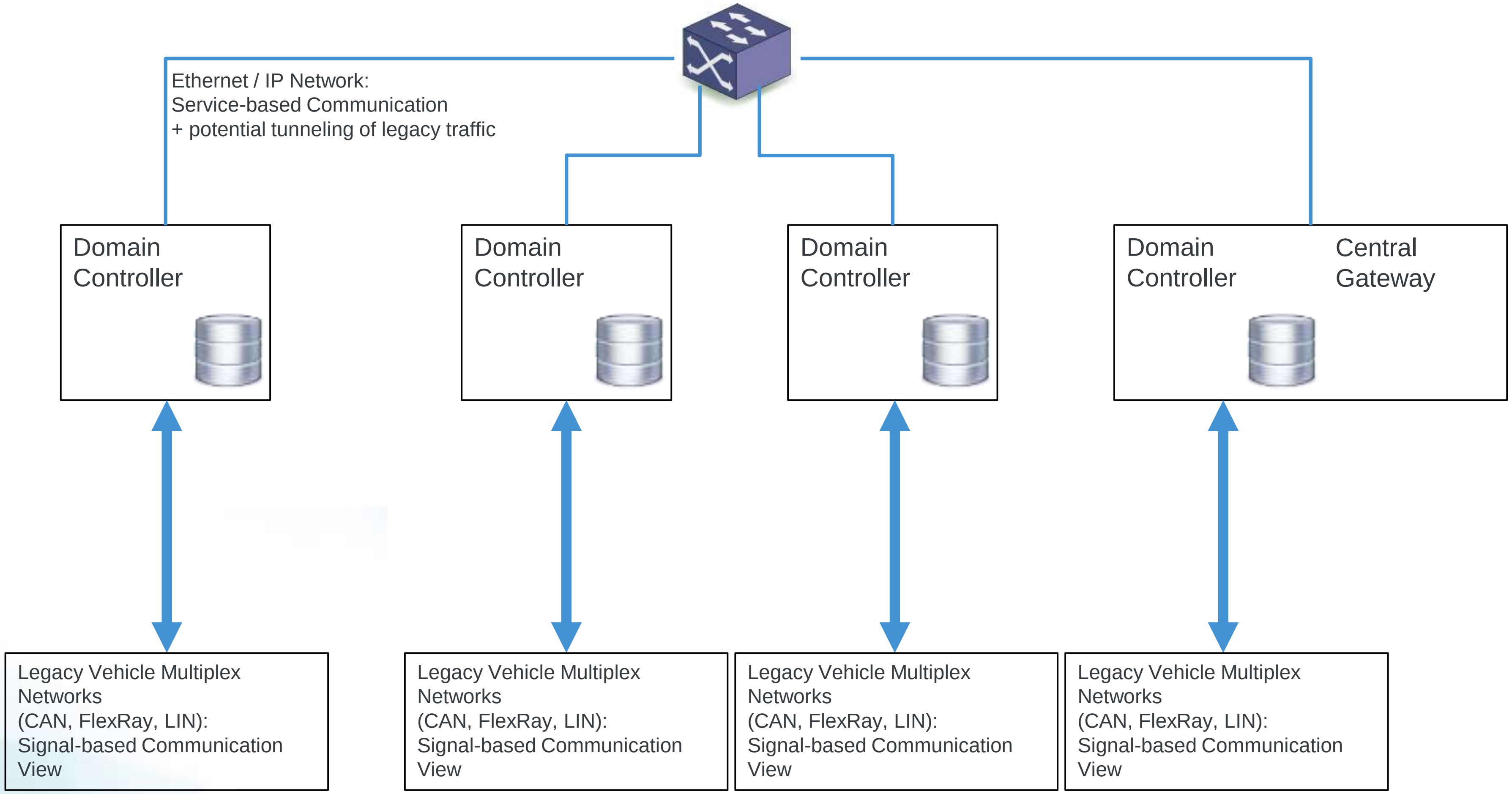


Today



202x

Pure Domain Network Communications Flow

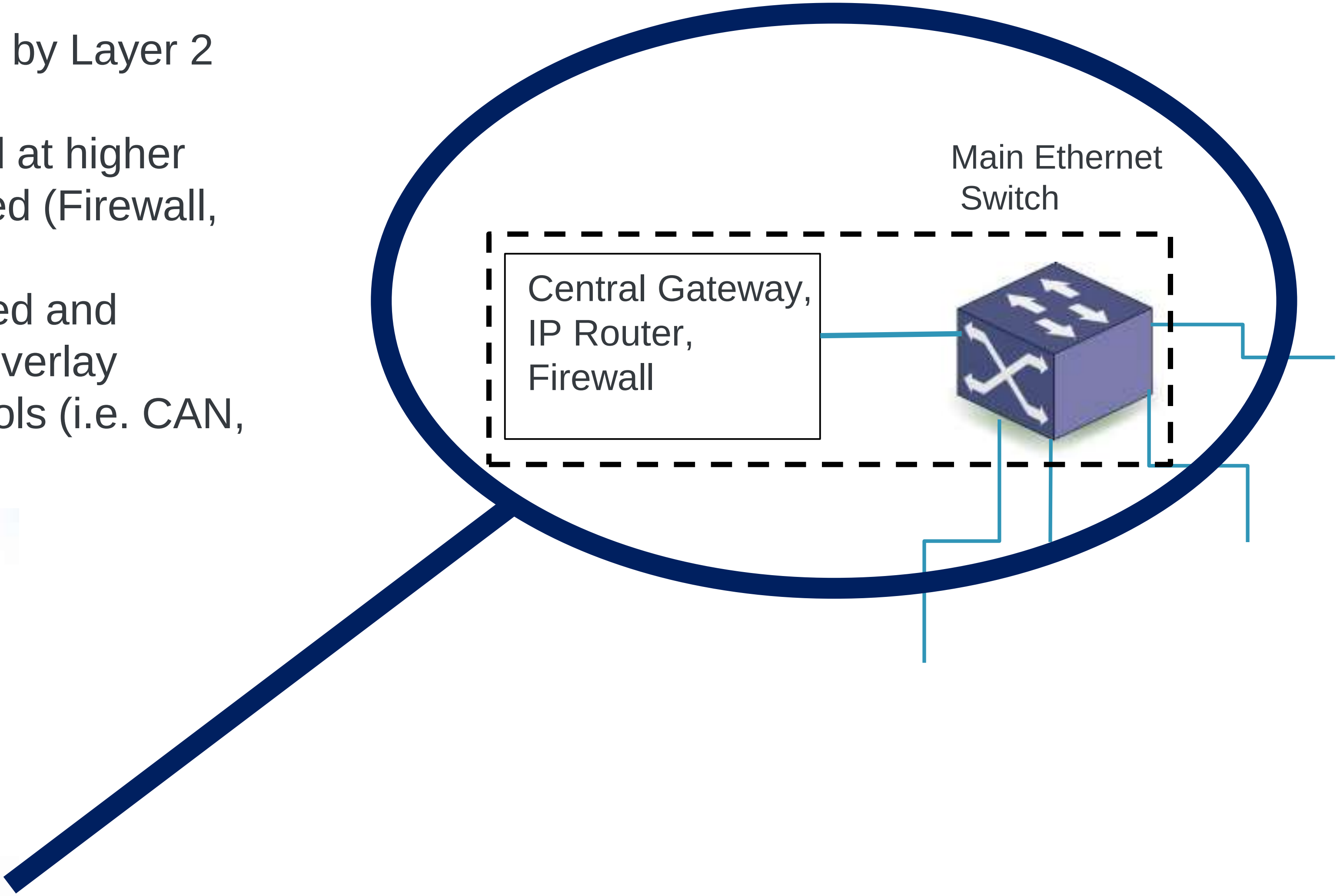


Ethernet / IP Network:
Service-based Communication
+ potential tunneling of legacy traffic

Domain Controller
Domain Controller
Domain Controller
Domain Controller
Central Gateway
Legacy Vehicle Multiplex Networks (CAN, FlexRay, LIN): Signal-based Communication View
Legacy Vehicle Multiplex Networks (CAN, FlexRay, LIN): Signal-based Communication View
Legacy Vehicle Multiplex Networks (CAN, FlexRay, LIN): Signal-based Communication View
Legacy Vehicle Multiplex Networks (CAN, FlexRay, LIN): Signal-based Communication View

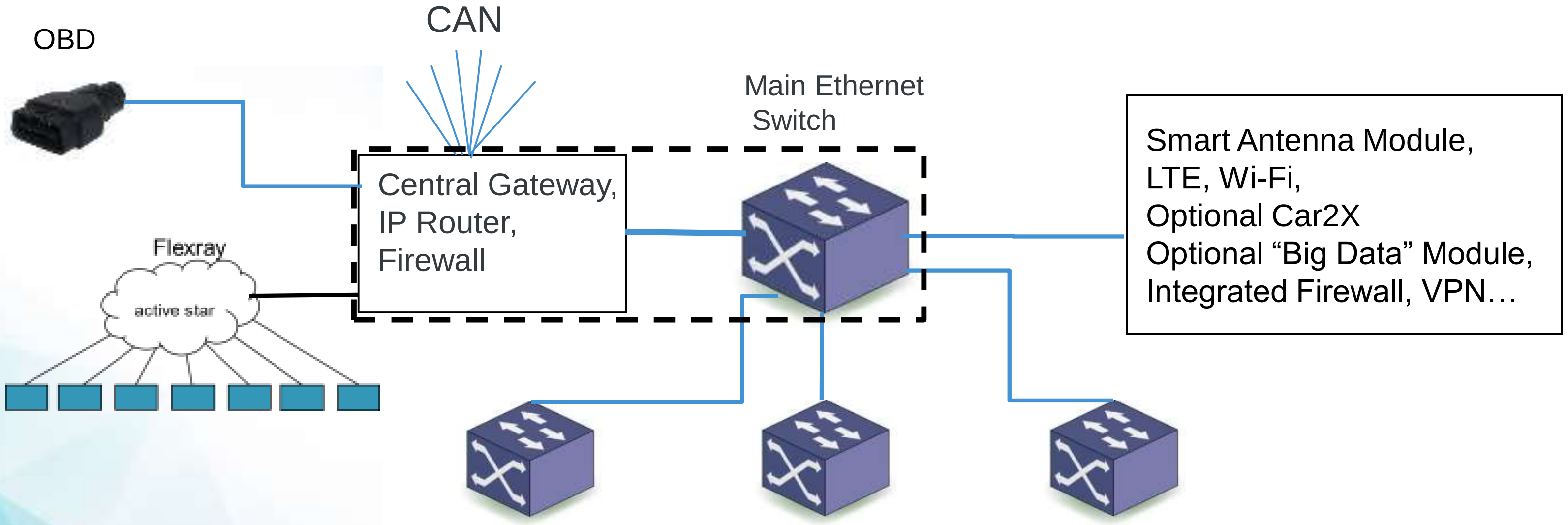
Central Gateway / IP Router / Firewall

- Domains are separated in VLANs
- Intra-Domain Traffic can be switched by Layer 2 Ethernet Switch
- Cross-Domain Traffic must be routed at higher layers (IP, Gateway, …) and inspected (Firewall, Stateful inspection)
- Due to different nature of signal-based and service-based communications, an overlay network of legacy automotive protocols (i.e. CAN, FlexRay) might be a better solution.



Alternative Legacy Automotive Overlay Network

- To simplify migration from existing vehicle network architecture an overlay network of the existing automotive interfaces (CAN, FlexRay, LIN) in the central Gateway could be a potential solution
- This reduces the complexity of network migration to only the Gateway
  - Legacy nodes talk e.g. CAN, FlexRay
  - New nodes talk IP, Service-based communication
- An additional benefit of this approach is, that for specific needs, ultra-low latency routing of legacy messages could be achieved
- This also provides a redundant communication path to avoid single point of failures


OBD
CAN
Main Ethernet Switch
Central Gateway, IP Router, Firewall
Flexray
active star
Smart Antenna Module, LTE, Wi-Fi, Optional Car2X Optional "Big Data" Module, Integrated Firewall, VPN…

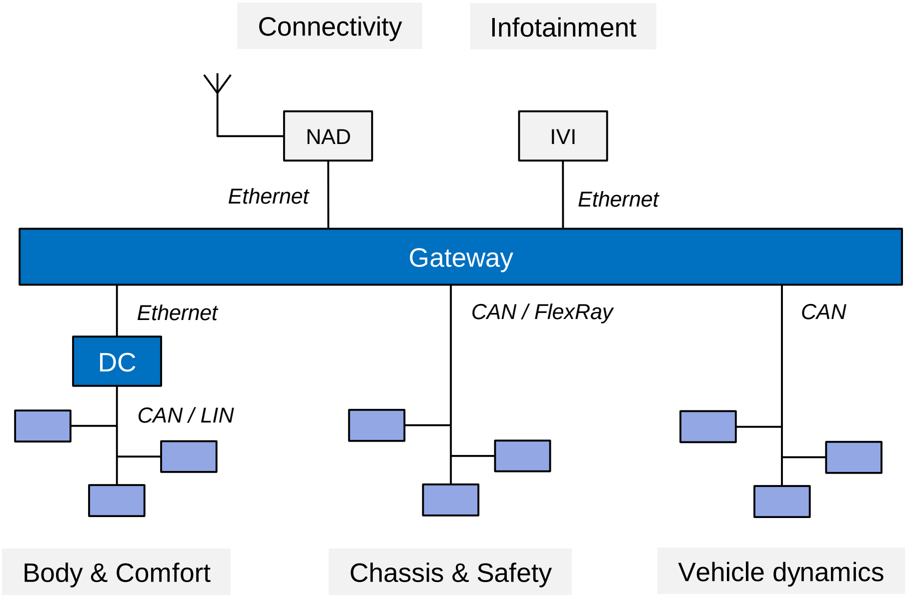
Gateway Evolution – Market Trends

Market Trends: Networking

- Move to a predominately **Ethernet backbone**
  - Bandwidth needs – Autonomous Driving Platforms
  - Domain controller approach – simplifies logistics of deploying vehicle platform
  - **IP Routing, VLAN & >L3 firewalling** to Isolate & Protect Ethernet domains
  - Diagnostics over IP (DoIP) usage widespread

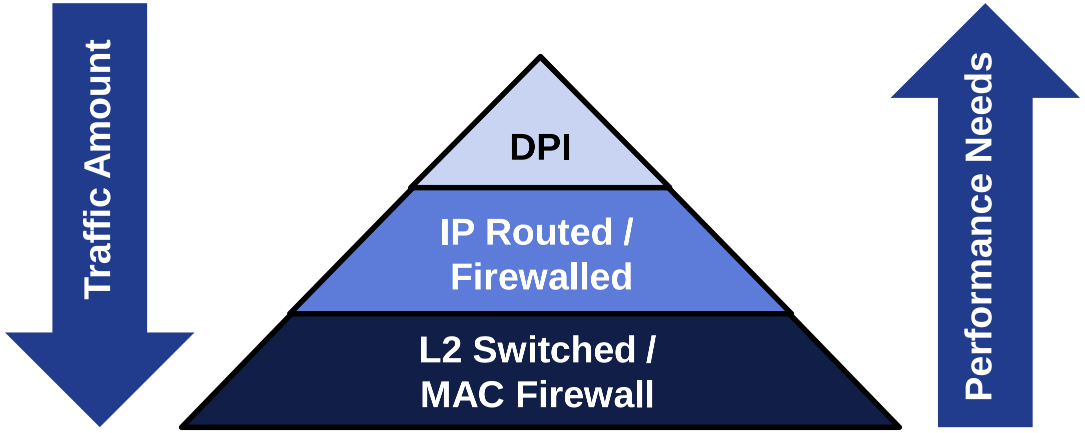
- Hybrid Approach during 2020 to 2025
  - Typical**: 3-5 Ethernet domains + 8+ CAN**

- # of CAN channels increasing
  - Isolation of increasing number of ECUs
  - Up to ~175 ECUs in some high-end vehicles!



Market Trends: Network Security

- Gateway is considered as a **central location for security.**
  - Policing vehicle information, monitoring traffic between networks
- **Growth of Ethernet**
  - Wider range of known attacks
  - Ways to protect:
    - Layered network hierarchy
    - Contextual firewalls, deep packet inspection (DPI), etc…
  - Firewalling & Security brings **significantly greater performance requirements** than CAN
  - Need for a processor with **network security in mind**

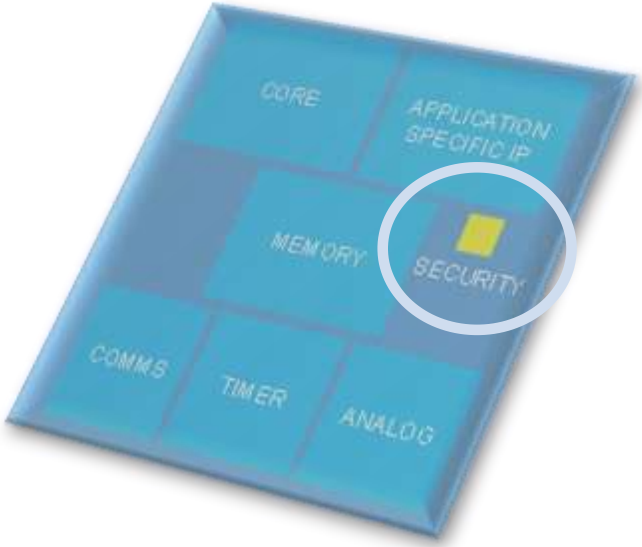


Market Trends: Processor Security

- Industry woke up to security following public hacks of 2015

- Need to **secure MCU/MPU from malicious attacks**
  - Taking control of the ECU
  - Stealing Intellectual Property

- **Connected services driving additional layers of security** in the gateway
  - Public Key handling acceleration, connecting through internet
  - Physical protection of keys guaranteed strong root of trust. Extremely high value keys that need protected

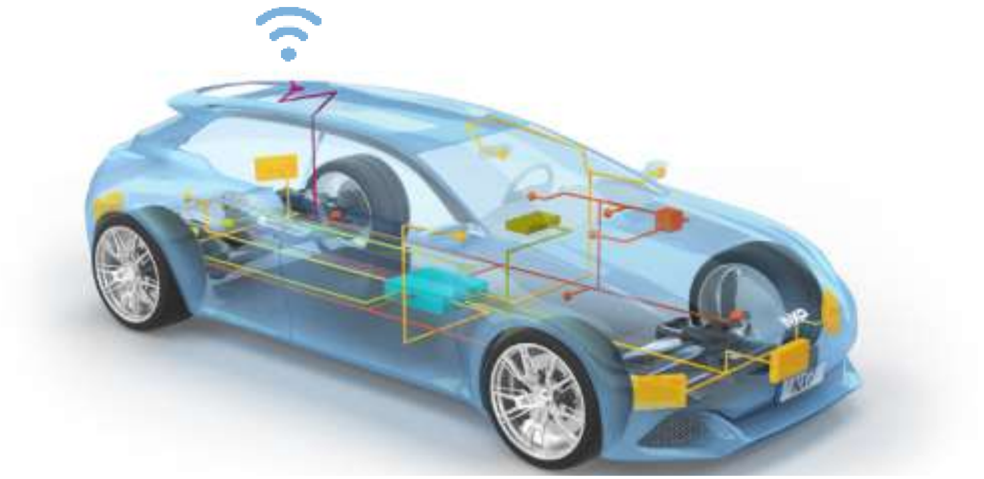


Market Trends: Over-The-Air (OTA)

- **Over-the-Air firmware/software updates** (to main ECUs) is a key trend in the industry

- **Trend to move OTA Management function in Gateway ECU**
  - Centralized management of OTA deployment in-vehicle
  - Interface to OEM servers
  - Security is paramount

- Utilizing OTA mechanism to **deploy new features via SW in field** (Agile SW deployment)
  - Build performance overhead into hardware
  - In-field, test & deploy new customer features as use cases emerge

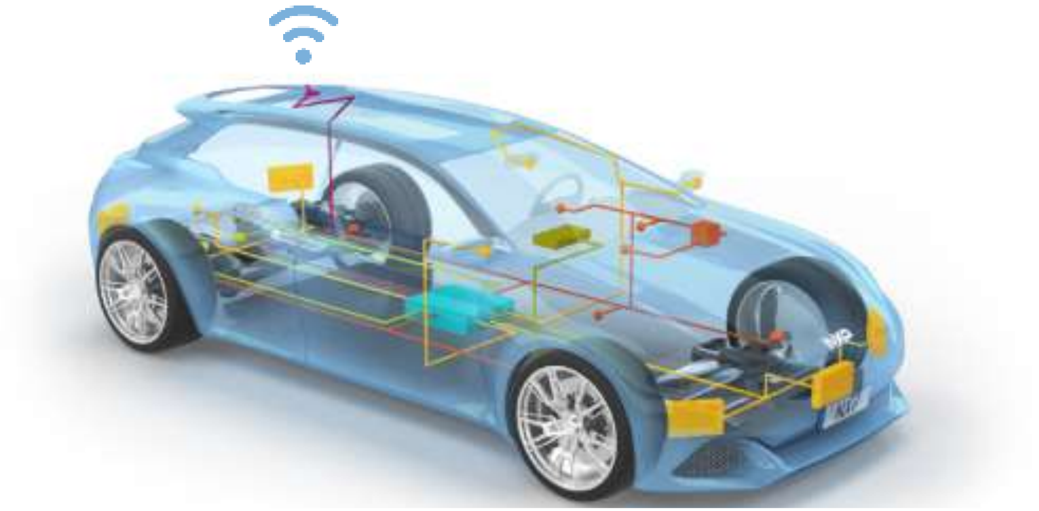


Market Trends: Connectivity

- **Trusted & untrusted connectivity**
  - Untrusted infotainment (IVI) system
  - Connected car vs In-Vehicle Network
  - New services being introduced to vehicles (e.g., OTA)

- See move to separation of connectivity
  - **Trusted: Gateway**
  - Untrusted/Consumer: IVI

- **Enabling new features:**
  - OTA Updates
  - Remote Diagnostics - Tester in gateway (Diagnostics over IP)
  - IoT Connectivity - Translation of raw data into rich information
  - Cloud Offload – e.g., Analytics, Modelling vehicle behaviour



Market Trends: Processing

- **1000’s of DMIPS performance** needed to support future gateway capabilities and new applications

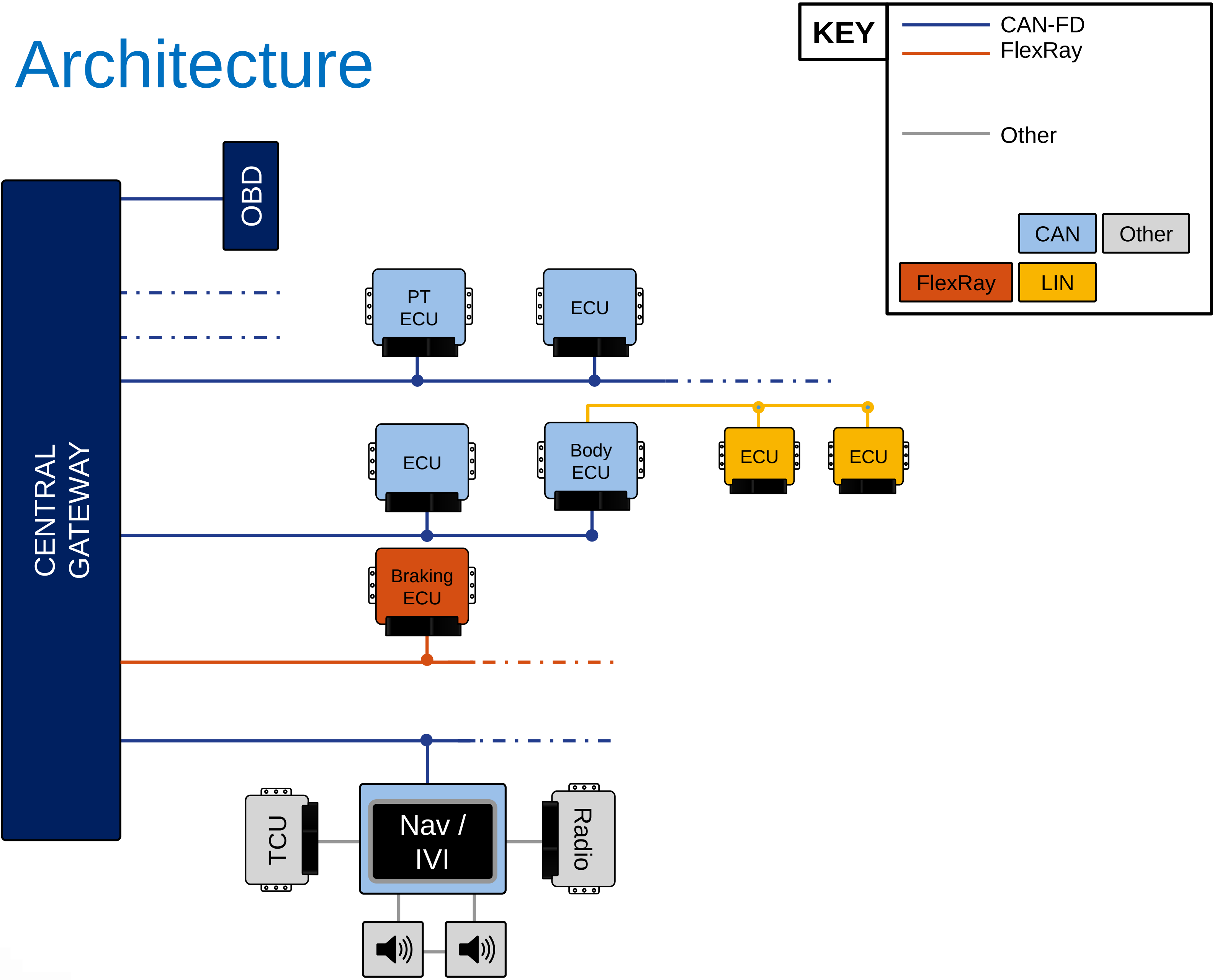
- **ECU consolidation**: Feature deployment by SW package rather than new ECU

- **Big Data Analytics**: Descriptive / Diagnostics / Predictive
  - Looking at security, safety & integrity of the vehicle & network

Gateway Evolution - Architectures

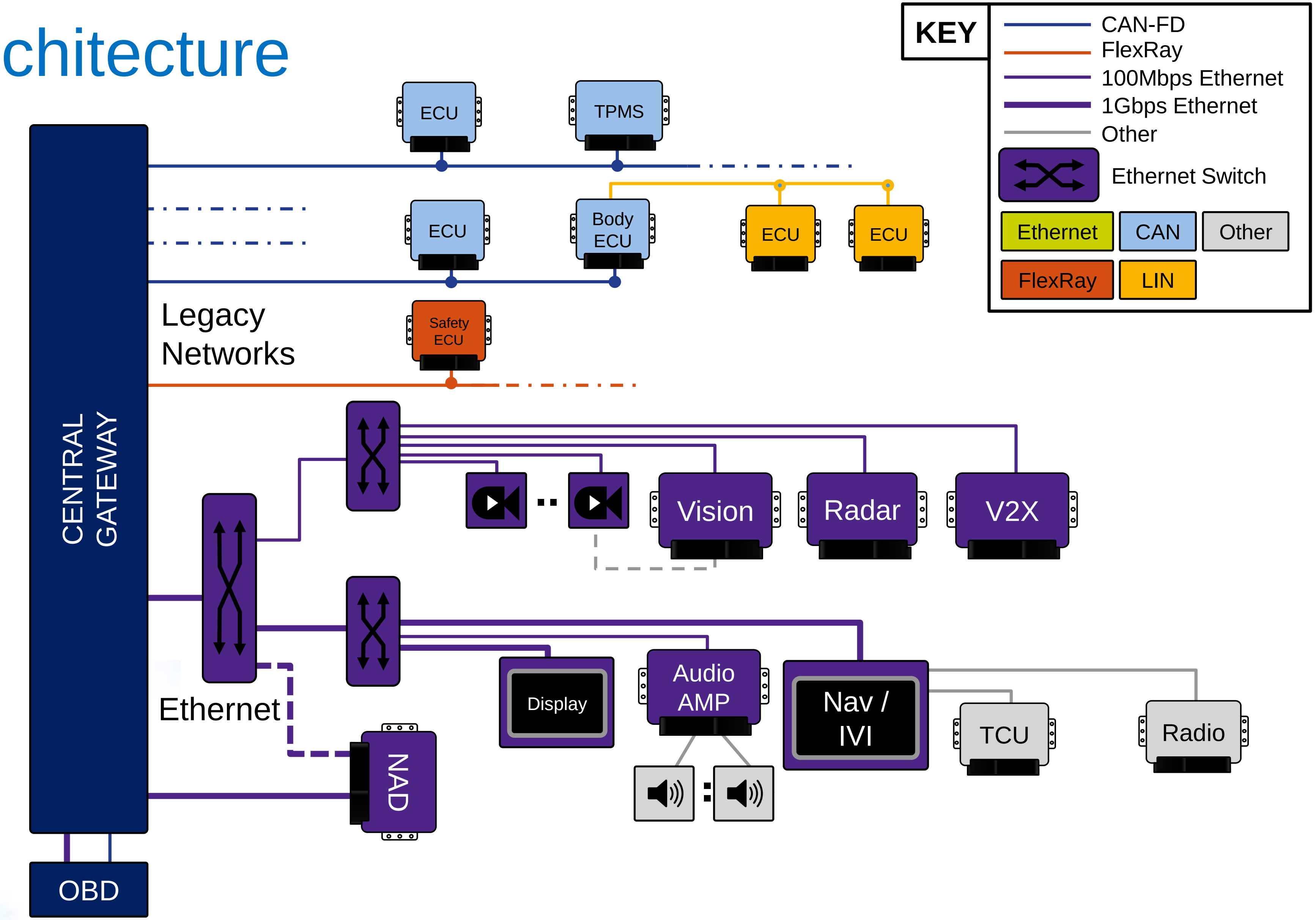
CAN Central Gateway Architecture

- Legacy Automotive Networks
  - Typically 3-8 CAN networks
  - Typically 1-2 FlexRay networks
- Increased bandwidth
  - but, small compared to consumer / networking world
  - Proprietary protocols for higher bandwidth (e.g. MOST)
- Physical Isolation
  - Functional domains
  - Safety / Non-safety
- Gateway role
  - Firewall internal traffic
  - Protocol translation



Hybrid Ethernet Architecture

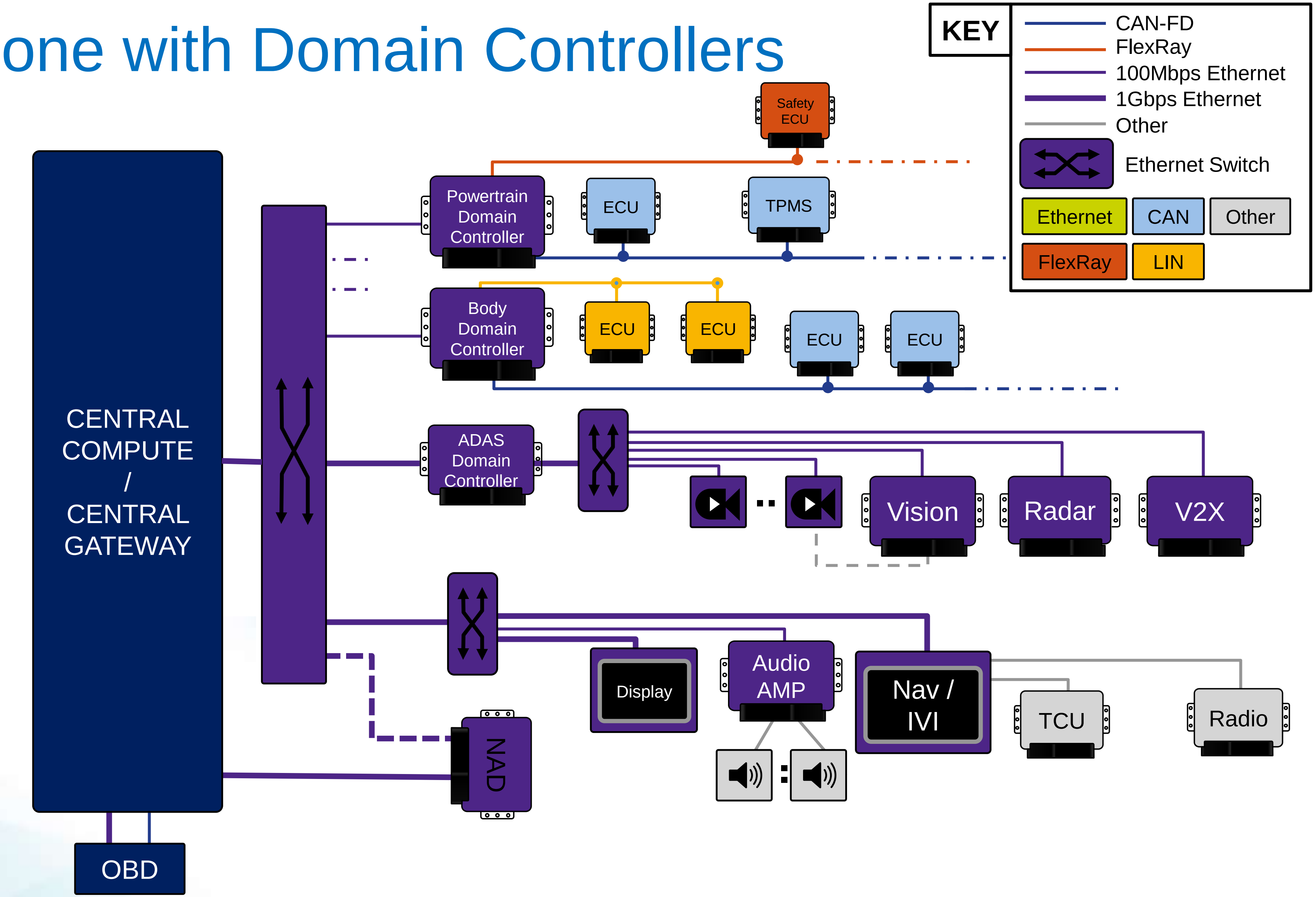
- Legacy + Ethernet Networks
  - CAN, FlexRay & Ethernet
- High-bandwidth Data
  - 100Mbit →1Gbit Ethernet
  - ADAS and Infotainment drive higher data rates
  - Improved ECU program time in factory
- Gateway role
  - Firewall internal & external
  - Efficient protocol translation
  - ECU consolidation
  - New apps & services



Ethernet Backbone with Domain Controllers

- **Ethernet Backbone with Domain Controllers**
  - ECU consolidation
  - Distributed gateway

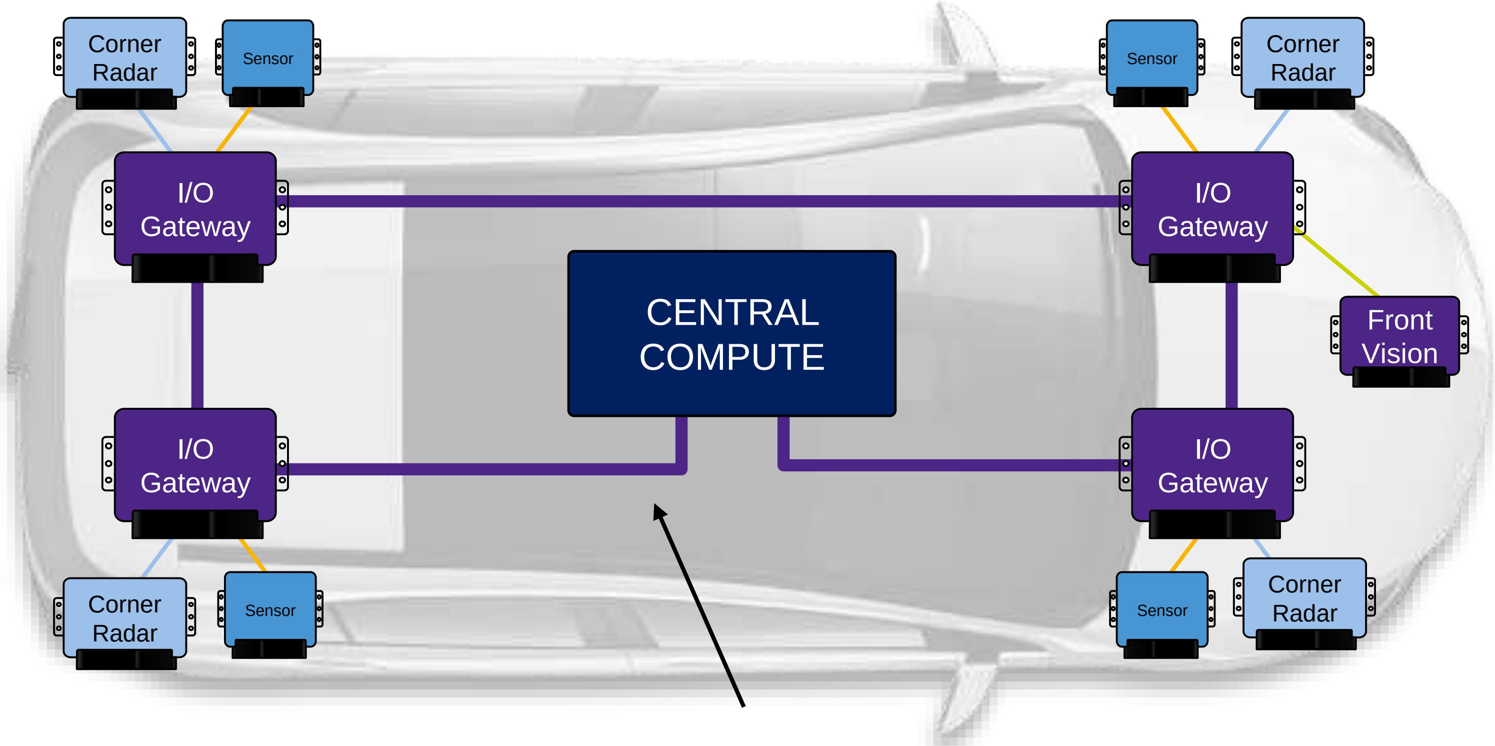
- Central Compute
  - Strategy / Decision making
  - Distributed vs Centralized



Central Compute Architecture

- Central Compute + I/O Gateways
  - No functional domains
  - Strategy for vehicle fully owned by Central Compute
- I/O Gateways connect Edge Nodes to Central Compute
  - Distributed processing
  - Optimize network utilization
- Benefits:
  - Network architecture optimised to vehicle topology
  - Less wires (less weight, power, cost)

‘Edge Nodes’
e.g. Radar ECU, Powertrain ECU

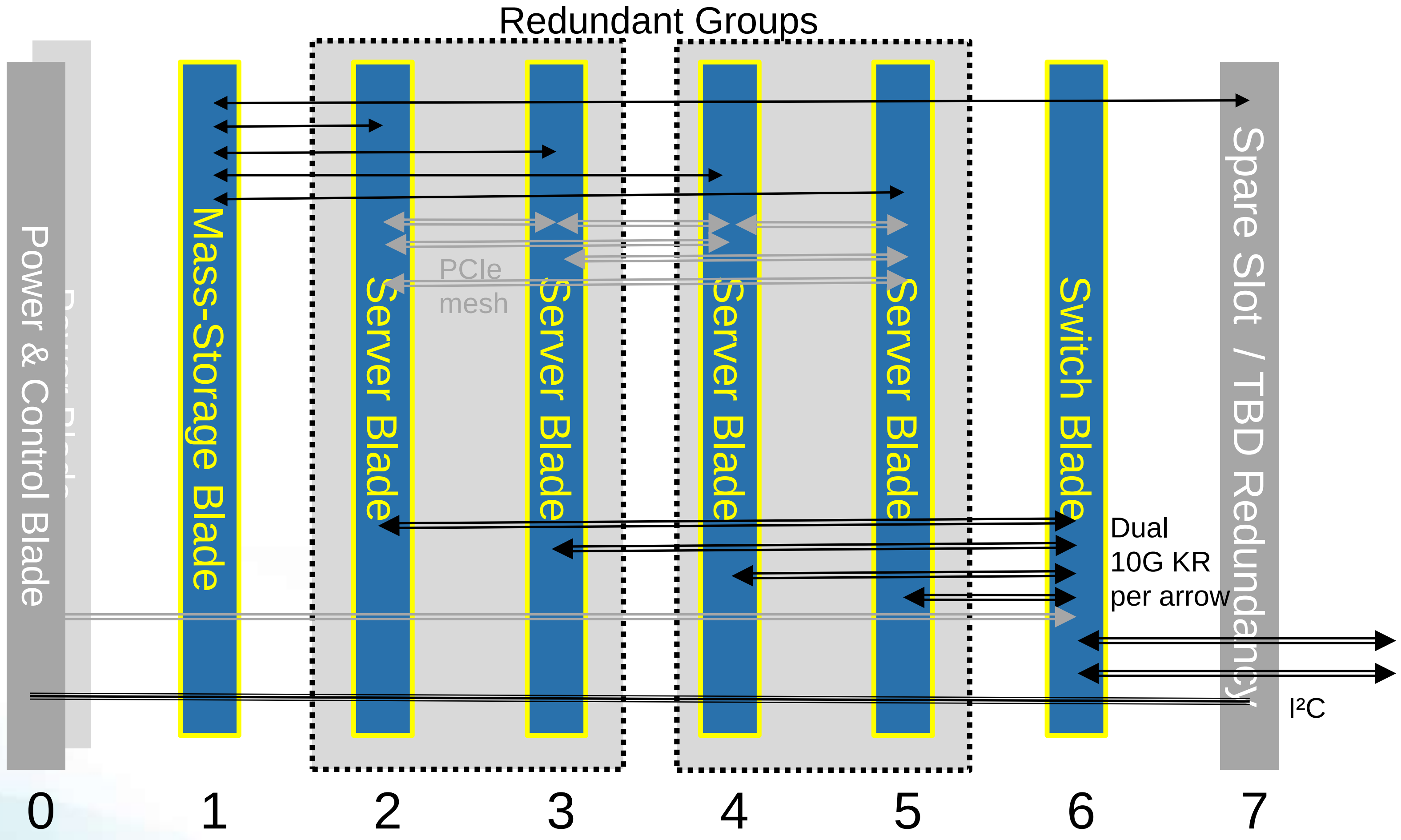


High Speed Ethernet Network (Mesh/Ring)
Optimised to vehicle topology for Reduced Wiring

Moving Towards a “Server in the Car”

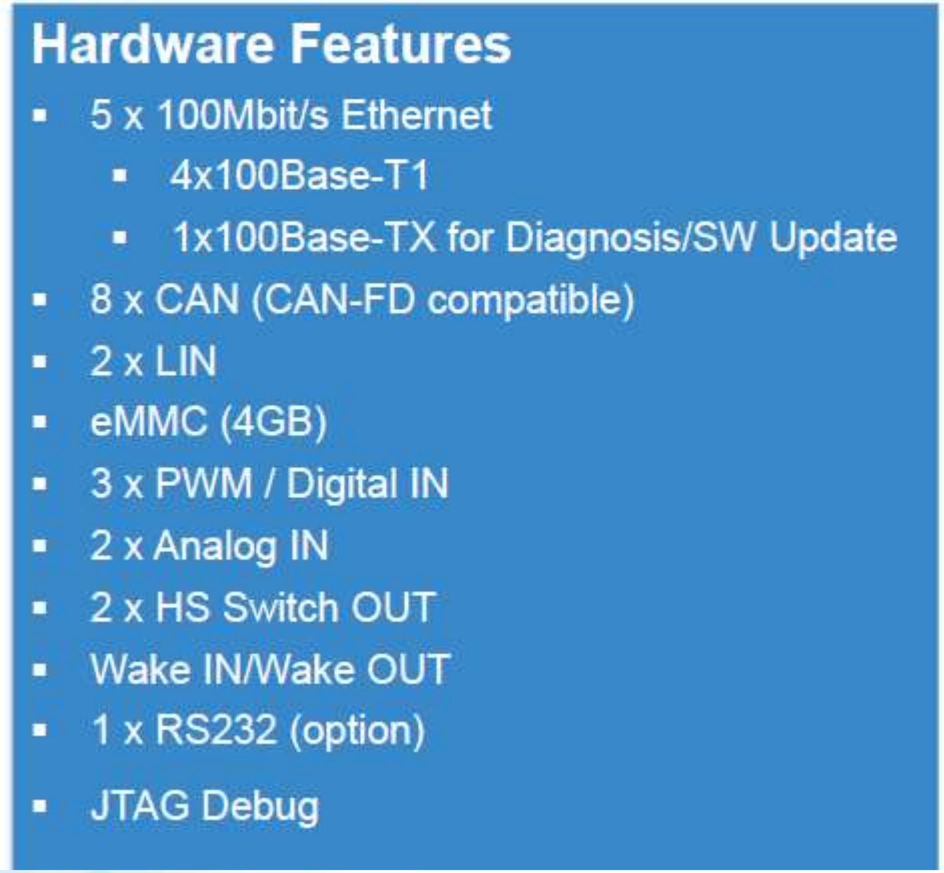
- Network Security
  - Intrusion Detection and Prevention
  - Firewall
- Applications server
- Integration of Cloud and Fog Services into the vehicle architecture
- Proliferation of PHY technologies
  - 100Base-T1 -> 1000Base-T1, 10 Mbps, 10 Gbps, 25 Gbps, 10GBASE-KR (802.3ap), …
- Communication Paradigms evolve
  - Service-based versus signal-based
  - Authentication
  - Encryption

Conceptual Vehicle Server Communications Links



NXP
Gateway Reference Solutions

NXP Secure Gateway Reference Design

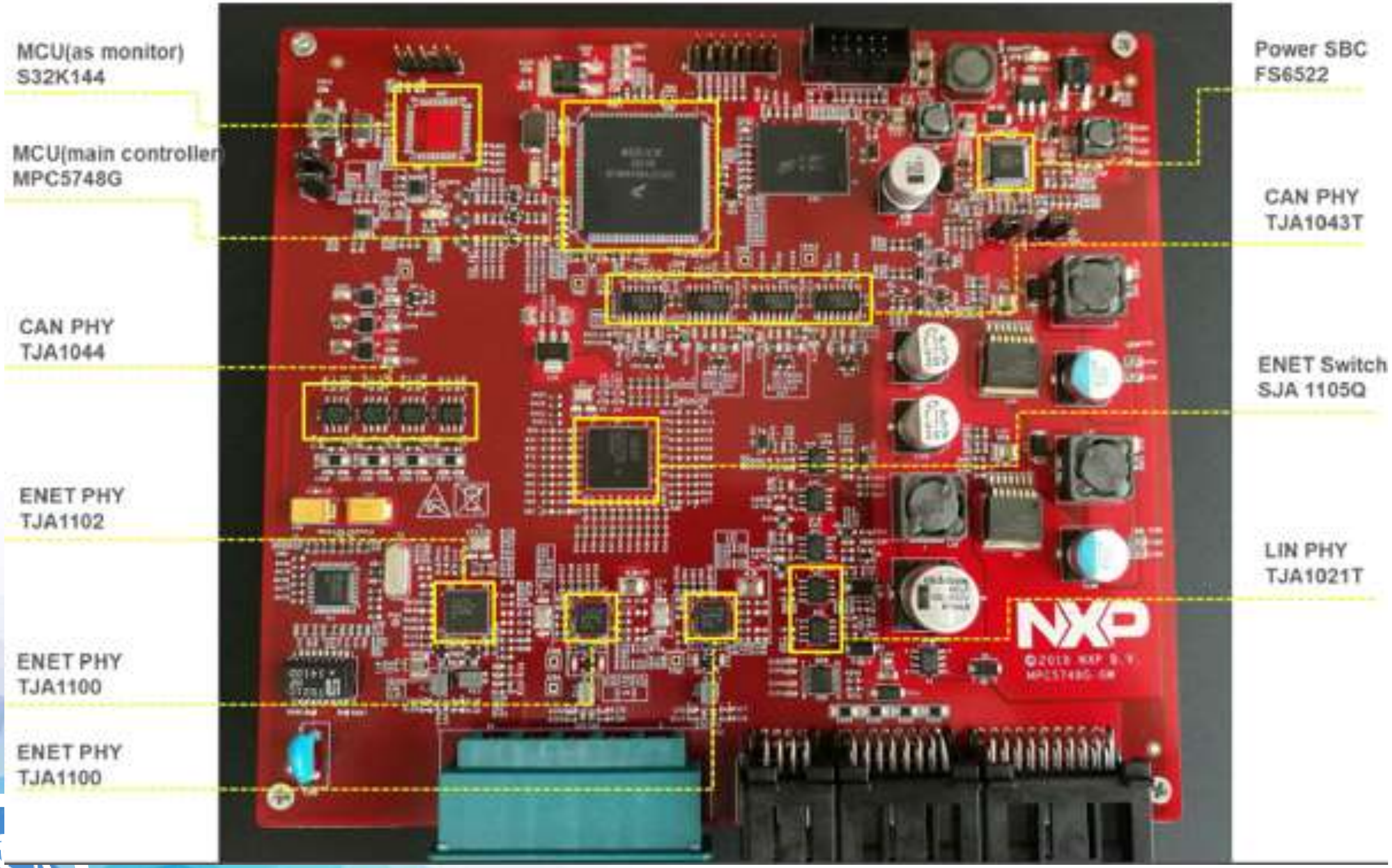


Hardware Features

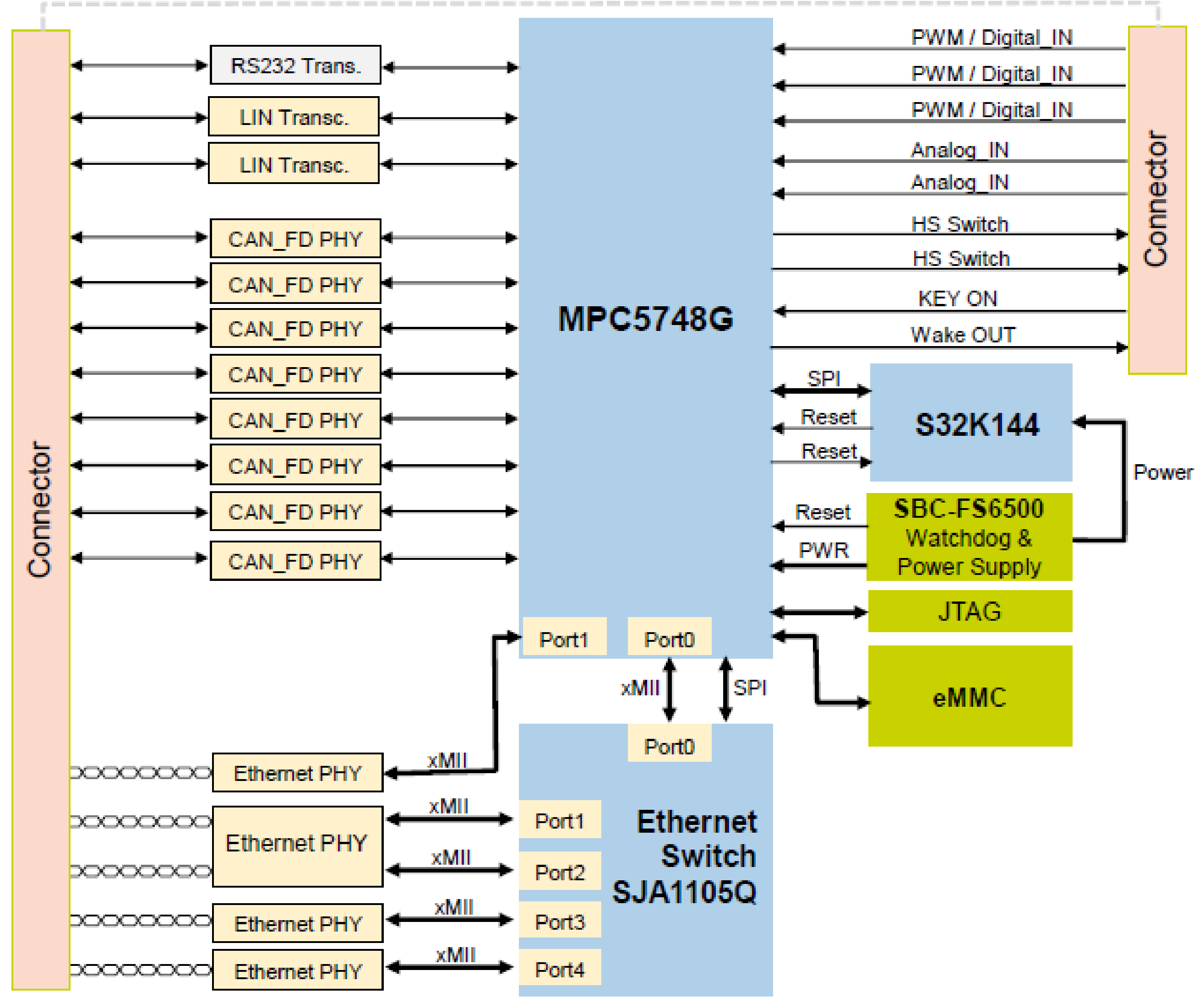
- 5 x 100Mbit/s Ethernet
  - 4x100Base-T1
  - 1x100Base-TX for Diagnosis/SW Update
- 8 x CAN (CAN-FD compatible)
- 2 x LIN
- eMMC (4GB)
- 3 x PWM / Digital IN
- 2 x Analog IN
- 2 x HS Switch OUT
- Wake IN/Wake OUT
- 1 x RS232 (option)
- JTAG Debug

Based on NXP MPC5748G Gateway Microcontroller

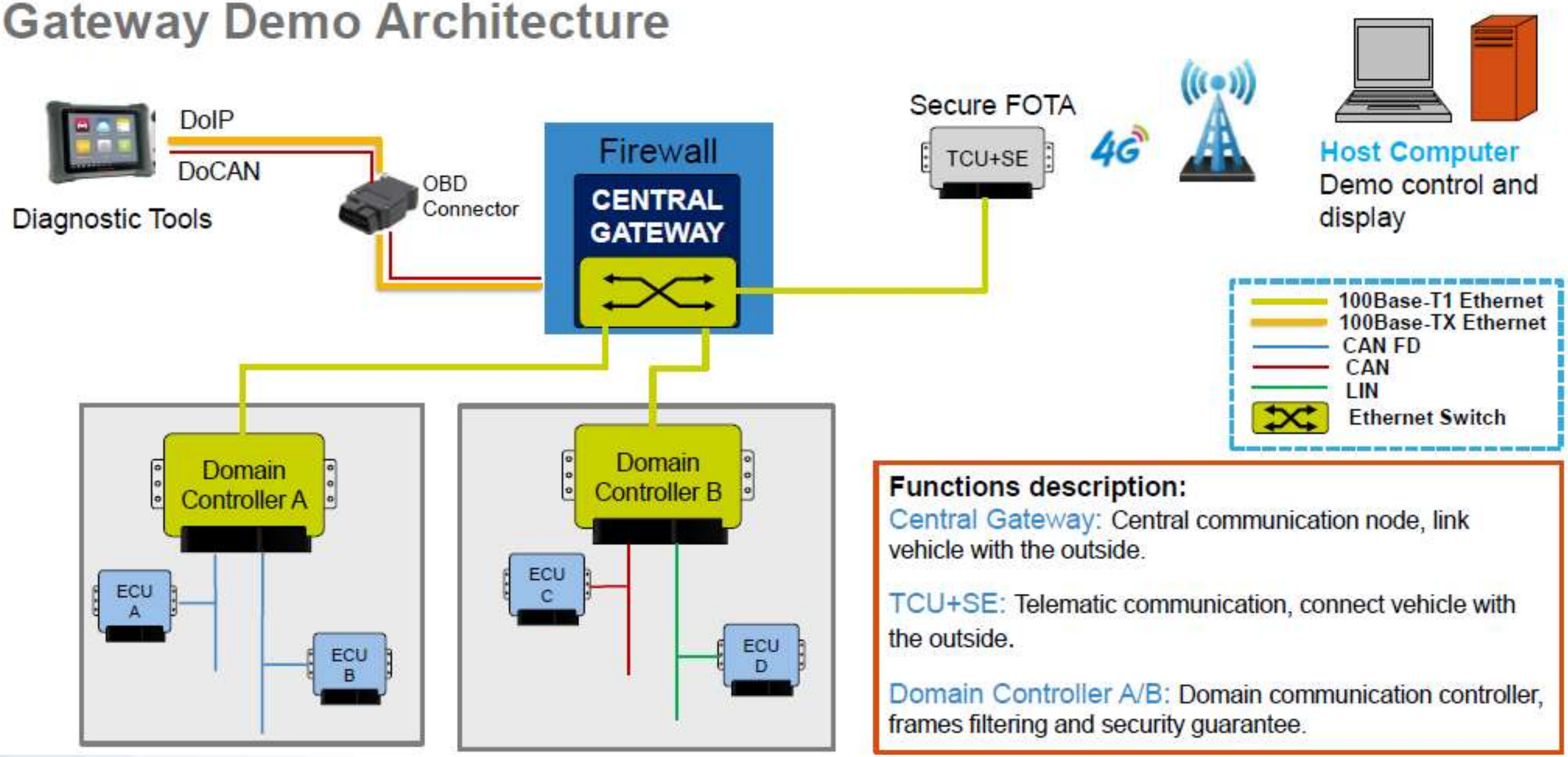
NXP Products on Secure Gateway Reference Design



NXP Secure Gateway Block Diagram



Gateway Demo Architecture



Functions description:

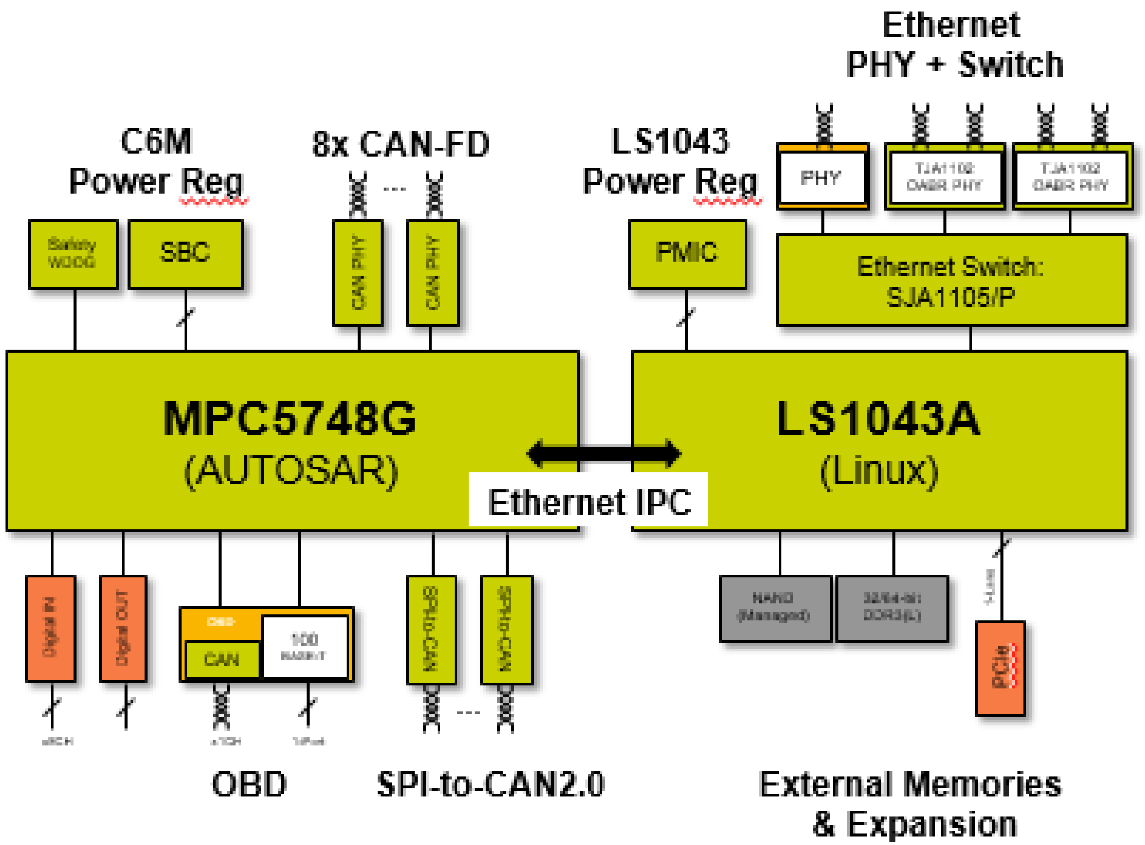
Central Gateway: Central communication node, link vehicle with the outside.

TCU+SE: Telematic communication, connect vehicle with the outside.

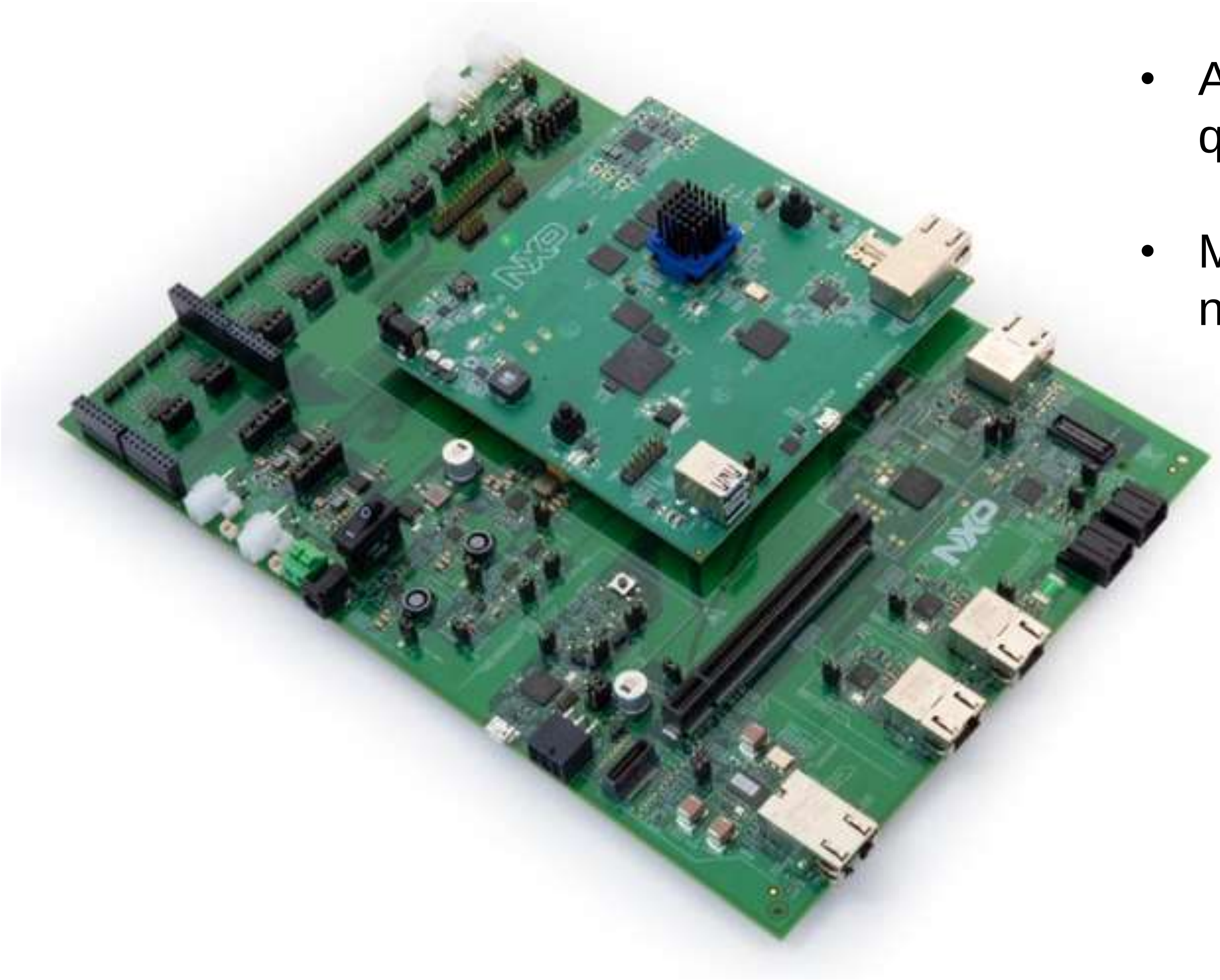
Domain Controller A/B: Domain communication controller, frames filtering and security guarantee.

Dual Chip Gateway Solution

- **Enables Next-Gen CAN-Ethernet Gateways**
  - Automotive Gateway + Network Processing (Gigabit Ethernet Packet Routing) + Applications
  - High-performance processing + IP acceleration
  - MPC5748G + LS1043A (MCU + MPU)
  - Available today
- **Feature Set**
  - CAN Signal Gateway (ASIL B)
  - 4x Arm Cortex-A53 (LS1043A)
  - Packet Forwarding Engine
- **OS Support**
  - AUTOSAR: Real-time CAN gateway
  - Linux: Ethernet routing, applications processing



Dual Chip Gateway Solution – Development Platform



- Available today – limited to qualified customer opportunities
- More information available in the near future

Summary

Summary

- Automotive Gateways are critical for providing secure communications between vehicle domains, but are evolving to provide more capabilities:
  - Over-the-Air Updates, Intrusion Detection, Analytics, Vehicle Health/Prognostics, Apps/Services…
- Multiple approaches to In-Vehicle Network architectures across carmakers and over the next decade:
  - No gateways → Central Gateway
  - Central Gateways + Domain Controllers
  - Central Compute → Server in the Car
- Gateways are evolving quickly to meet new demands driven by vehicle electronics: connected car, infotainment, ADAS/autonomous driving,...
  - More performance, security, connectivity, higher bandwidth, safety
- NXP is leading the way in / vehicle network processors to help drive the Gateway Evolution and enable carmakers' innovations

For More Information

NXP Central Gateway Site

NXP Secure Gateway & In-Vehicle Networking

SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com

NXP, the NXP logo, and NXP secure connections for a smarter world are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2018 NXP B.V.