Automotive Gateway: A Key Component to Securing the Connected Car

Introduction

Building vehicles with gateways – electronic devices that enable secure and reliable communications among a vehicle's electronic systems – is an emerging trend in the automotive industry. An increasing number of electronic systems contribute more than 90% of modern vehicle innovations and features. This growth is transforming vehicle network architectures with automotive gateways that provide seamless communications between heterogeneous vehicle networks and address data bandwidth, security, and safety challenges.

Connected cars are potential targets for remote attacks, and without proper protection, they can be compromised, resulting in loss of control, driver injury, and costly litigation. Fortunately, gateway security mechanisms can help greatly reduce the risk of cyberattacks to maximize driver safety, as well as prevent vehicle theft and loss of intellectual property. An automotive gateway serves a critical role in vehicle security, in addition to performing data routing functions, and supporting new, vehicle-wide applications.

What Is a Gateway?

Increased consumer demand for greater vehicle functionality is spurring more complex electronics in cars with an increased number of computers called Electronic Control Units (ECUs) with different network interfaces. Modern vehicles can integrate over 100 ECUs connected over multiple networks such as CAN (Control Area Network), LIN (Local Interconnect Network), FlexRay, and Ethernet.

The heterogeneous vehicle networks have unique protocols with a wide range of data rates. LIN is used for low-speed applications like sensors and actuators (20 kbps), CAN is used for medium-speed applications, including most ECU-to-ECU communications (1-5 Mbps), FlexRay is used for real-time, safety-critical applications (10 Mbps), and Ethernet is used for high-speed applications such as infotainment and advanced driver-assistance systems (ADAS), as well as wireless interfaces (3G/4G/future 5G, BT, Wi-Fi, V2X) (100 Mbps to gigabit speeds).

A gateway is a central hub that securely and reliably interconnects and processes data across these heterogeneous vehicle networks. It provides physical isolation and protocol translation to route data between functional domains (powertrain, chassis and safety, body control, infotainment, telematics, ADAS) that share data to enable new features. Gateways allow engineers to design more robust and functional vehicle networks that can enhance the driving experience.

Vehicle manufacturers (OEMs) are highly motivated to create new features to differentiate themselves from competition. A gateway is essential for enabling autonomous driving which requires secure connectivity and high-bandwidth communications across functional domain ECUs. Being central to the vehicle networks, the gateway is also ideal to support vehicle-wide applications such as Over-the-Air (OTA) updates and vehicle analytics with secure communications to OEM servers (cloud).

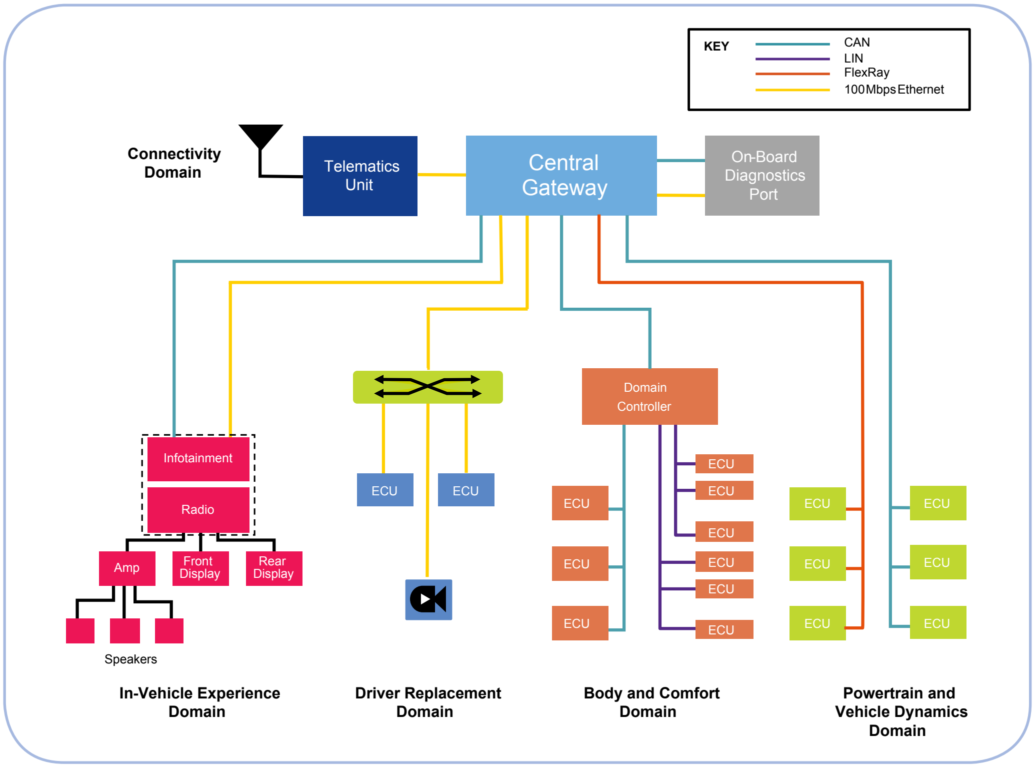

Fig. 1 Automotive Gateway Bridges Functional Domains and Heterogeneous Vehicle Networks

Gateway Capabilities

The main function of a gateway is to provide secure, seamless communications between networks and ECUs, including bridging between the many internal networks of the vehicle and the external networks of the outside world. The smooth transfer of data is essential for ensuring ECUs have the information they need for proper vehicle operation, so the gateway must provide any-to-any network communications and with low latency and jitter.

There are many gateway capabilities that are required to accomplish the seamless communications. The following table provides a summary of key gateway capabilities (not an exhaustive list).

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

Key Gateway Capabilities Summary

A gateway in a connected car is ideal for managing remote OTA updates of ECUs' firmware. The few vehicles that support OTA updates today typically only update the infotainment or telematics systems. OTA updates through a gateway, which interfaces with all vehicle functional domains, allow OEMs to remotely fix/prevent vehicle problems, address security vulnerabilities, and enable new features that improve the user experience and can generate revenue. NXP has optimized gateway processors to support efficient, and flexible OTA updates. The NXP whitepaper "**Making Full Vehicle OTA Updates a Reality**" provides more details.

Speaking of Security ...

Addressing the fast-growing automotive market requirements for security is an increasingly complex challenge. Automotive networks can be targets of cyberattacks – especially legacy networks like CAN that were not designed with security in mind – making them vulnerable to forged messages and jamming attacks. Connected cars' external wireless interfaces present another attack vector that increase security risks further. Hackers could extract assets such as private information or cryptographic keys or impact the operation of vehicle by exploiting implementation vulnerabilities. These security risks can in part be mitigated with a Secure Gateway as part of a multi-layer security architecture. NXP delivers a comprehensive, **multi-layer approach for automotive security**. The NXP whitepaper **"Cybersecurity for ECUs: Attacks and Countermeasures"** is also an excellent reference that dives into more details and guidance on security protections for ECUs, including gateways.

The Secure Gateway layer acts as a firewall that controls access from the external interfaces (such as the Internet) to the vehicle's inner network, and controls which nodes in the vehicle's network can communicate with each other. It also provides functional domain isolation; for example, between an untrusted infotainment system and trusted safety-critical systems. The Secure Processing layer provided by NXP gateway processors features secure boot and real-time integrity checking schemes to guarantee code is authentic, trusted, and unaltered, and provide an embedded Hardware Security Module (HSM) for cryptography and secure key management.

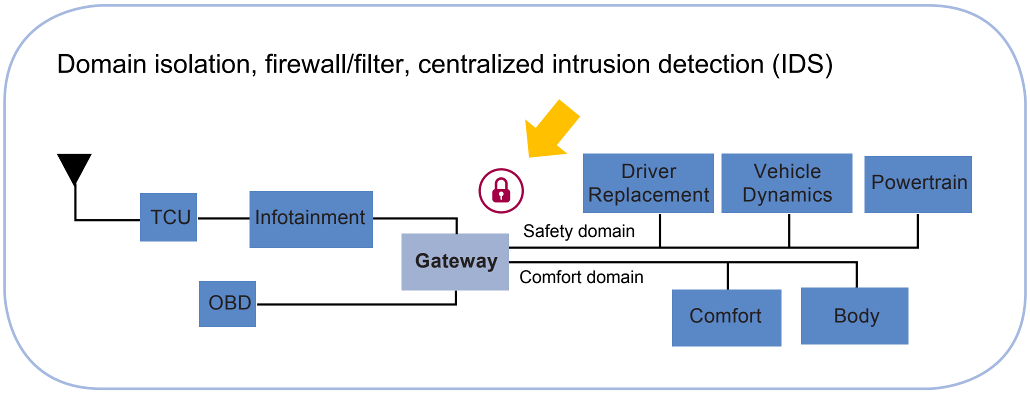

Fig. 2 Secure Gateway and Processing

Security mechanisms also protect the interfaces and communications through message authentication to validate senders, encryption to protect data integrity and privacy, and traffic monitoring for intrusion detection to prevent externally-induced hazards that can impact safety. It is crucial that a gateway has a trusted execution environment that is physically isolated, has secure memory, and is resistant to physical attacks to maintain the security integrity.

Looking to the Future

Connected cars are like mobile devices: always-connected devices with increasing complexity, performance, and security requirements. Future autonomous vehicles' ECUs must work together to sense, process, and act to drive. This requires moving and processing a tremendous amount of data securely between ECUs. Connected cars will continue to drive higher data bandwidth requirements with 5G cellular. There is a trend to move to multi-gigabit Ethernet for internal networking, and eventually as a backbone for communications between domains. The transition to Ethernet may distribute gateway functionality into domain controllers (DCs) that provide localized processing/control and routing data between legacy automotive interfaces, while a central gateway routes Ethernet data packets between domains within the vehicle. Gateways will continue to evolve to meet these architectural changes and challenges to perform capably (bandwidth, latency, performance, security). NXP is leading the way to enable next-generation automotive gateways with optimized solutions.

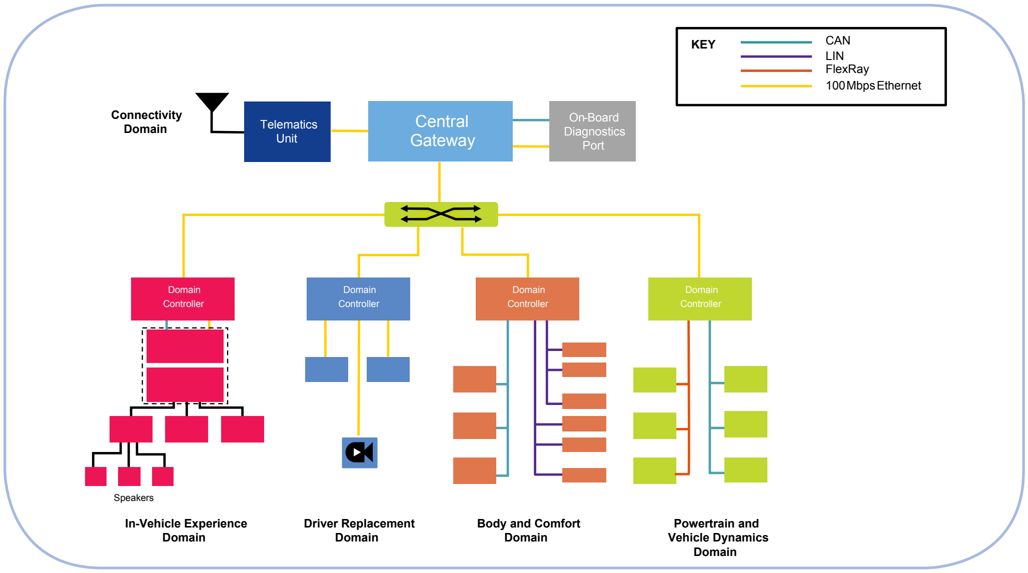

Fig. 3   Evolution to Central Gateway with Ethernet Backbone and Domain Controllers

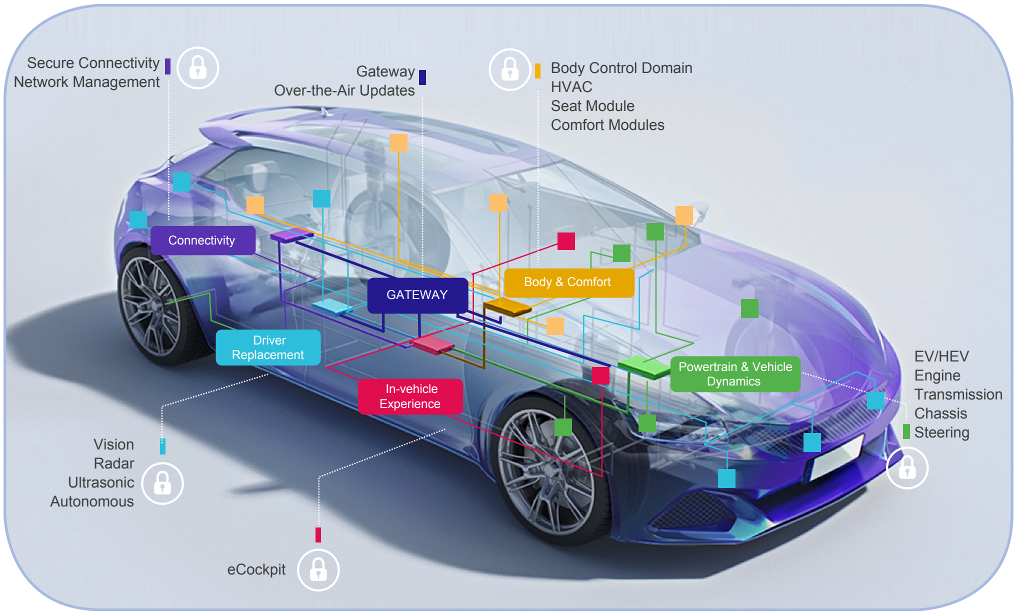

Fig. 4   Central Gateway Interconnects Functional Domains

NXP and the Connected Car

NXP Semiconductors is the world leader in vehicle network (gateway) processors and In-Vehicle Networking (IVN), providing about half of all network connections found in a new car. CAN, LIN, FlexRay, and Ethernet networks with robust processors tie everything together, ensuring reliable, safe, and secure communication between the electronics inside the vehicle. IVN systems and gateways must be easy to design, using products with characteristics that meet real network needs. High integration levels reduce component count, reduce robustness in the challenging vehicle environment, and reduce system cost. NXP offers complete system solutions and reference designs for gateways with vehicle network processors, secure elements, network transceivers, switches, and power management devices optimized to work together.

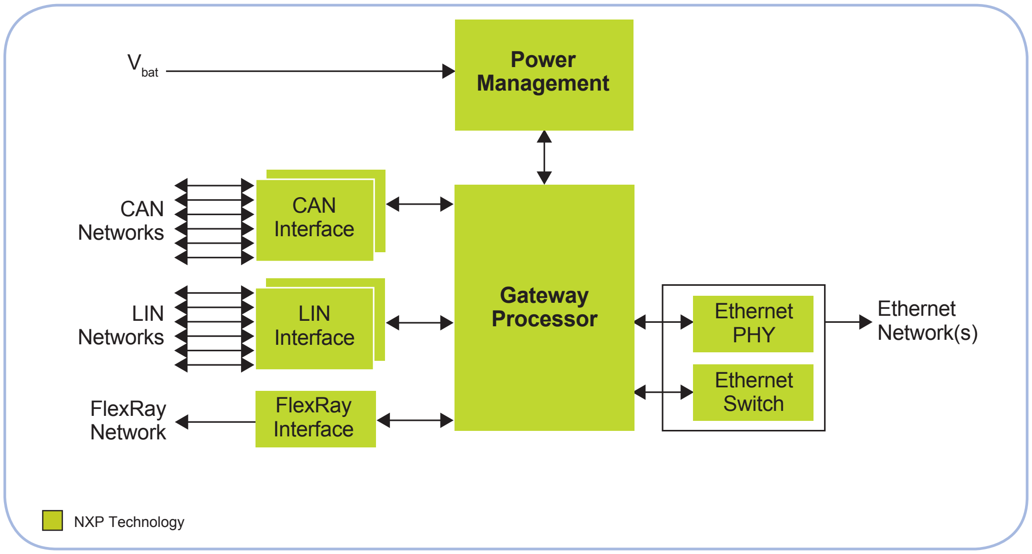

Fig. 4 NXP Offers Complete Gateway Solution

For more information, please visit the NXP website at: **https://www.nxp.com/gateway**

How to Reach Us:

Home Page: **www.nxp.com**
Web Support: **www.nxp.com/support**

USA/Europe or Locations Not Listed:
NXP Semiconductor
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.nxp.com/support

Europe, Middle East, and Africa:
NXPHalbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.nxp.com/support

Japan:
NXP Japan Ltd.
Yebisu Garden Place Tower 24F,
4-20-3, Ebisu, Shibuya-ku,
Tokyo 150-6024, Japan
0120 950 032 (Domestic Toll Free)
www.nxp.com/jp/support/

Asia/Pacific:
NXP Semiconductor Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@nxp.com