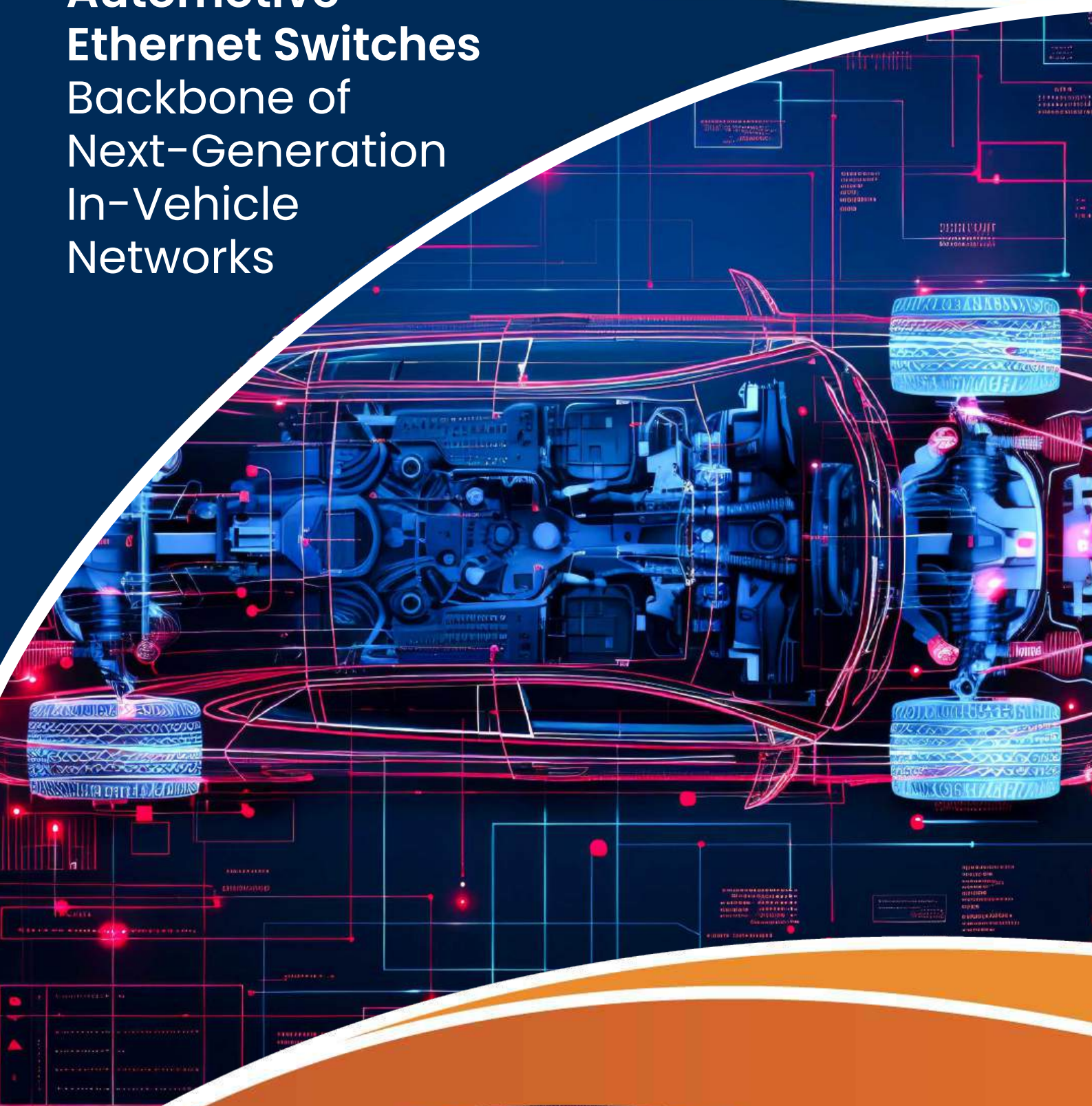
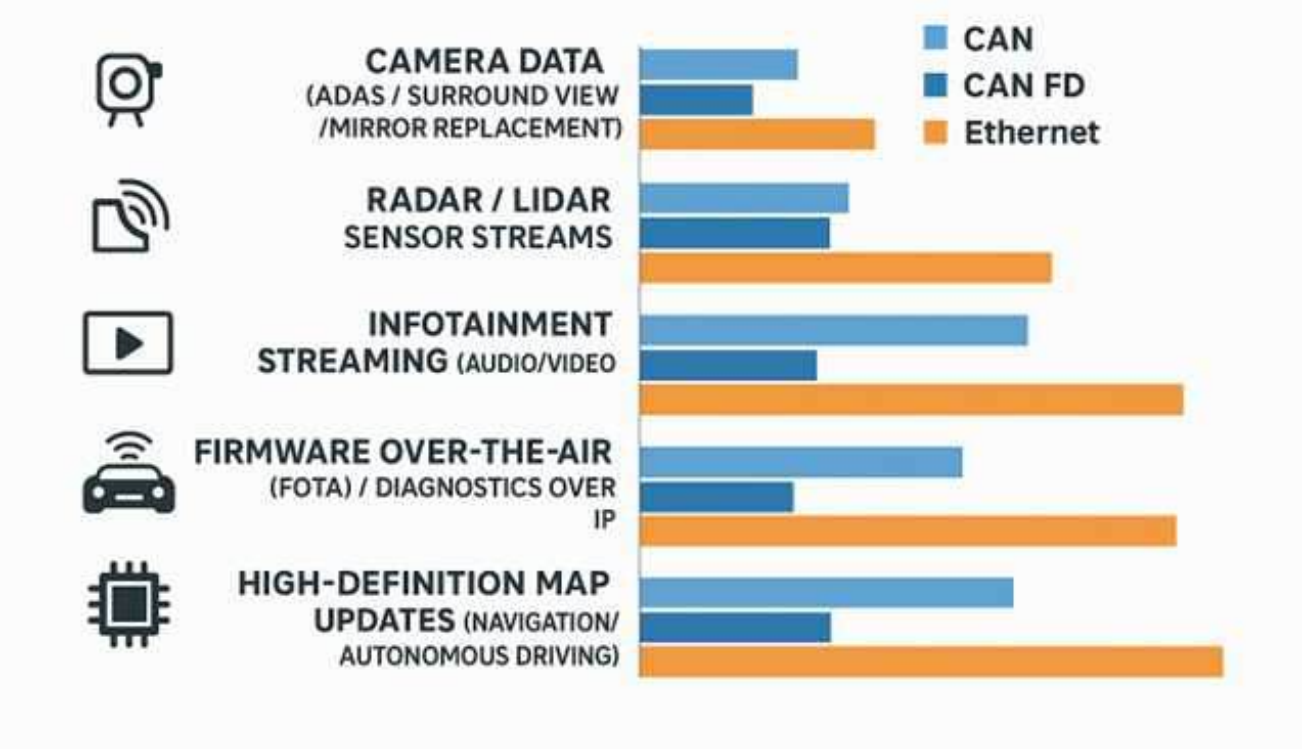
TESSOLVE
A **HERO ELECTRONIX** VENTURE

Automotive Ethernet Switches Backbone of Next-Generation In-Vehicle Networks



1. Introduction

Traditional automotive networks rely on technologies like CAN, LIN, and MOST, which are reliable but were developed for centralized architectures. The rapid transformation of vehicles having software-defined vehicle systems into highly connected vehicle systems, intelligent edge-compute, integrated advanced driver-assistance systems (ADAS), high-resolution cameras, radar, lidar, and OTA updates were fundamentally demands High-bandwidth with legacy bus and lower latency to meet In-vehicle communications requirements and Traditional network technologies can no longer sustain the escalating data volumes and latency constraints.



Future SDV networking system emerged with Automotive Ethernet as the de facto communication backbone for next-generation vehicles. These Ethernet switches play a pivotal role in aggregating and routing data across multiple zones, enabling efficient communication between local ECUs and centralized compute platforms capable of delivering scalable bandwidths from 100 Mbps up to 10 Gbps, deterministic communication through Time-Sensitive Networking (TSN), and compatibility with both legacy and IP-based architectures. Its ability to unify disparate vehicle domains—such as powertrain, body, chassis, infotainment, and ADAS—over a single standardized protocol significantly simplifies network design and reduces wiring complexity.

2. Evolution of In-Vehicle Networking

For decades, in-vehicle communication has relied on multiple domain-specific networks, each optimized for a particular function. The **Controller Area Network (CAN),** introduced in the 1980s, became the industry standard for powertrain and body control applications, offering robust and deterministic delivery for low-speed control signals. The Local Interconnect Network (LIN) is a low-cost sub-bus used for non-critical parts like window regulators, mirrors, and seat controls. Later, **FlexRay** enabled faster, predictable communication for safety-critical functions such as braking and steering, while MOST (Media Oriented Systems Transport) was designed for multimedia and infotainment applications.

The growing complexity of distributed ECUs has also increased wiring harness weight and cost. Each legacy bus requires dedicated cable and gateways for inter-domain communication, creating bottlenecks and diagnostic challenges. OEMs seeking to reduce vehicle weight, improve energy efficiency, and simplify network maintenance began exploring Ethernet as a universal backbone.

Automotive Ethernet emerged as the logical evolution — leveraging proven IEEE 802.3 Ethernet standards while introducing automotive-specific extensions to address electromagnetic compatibility (EMC), deterministic behavior, and robustness. The introduction of single-pair Ethernet (SPE) technologies such as **100BASE-T1, 1000BASE-T1, and 10GBASE-T1** has enabled high-speed, full-duplex communication over lightweight, unshielded twisted pairs suitable for harsh automotive environments.

Driven by industry initiatives like the **OPEN Alliance** and standardization under **IEEE** and **AVnu,** Automotive Ethernet has evolved into a scalable, interoperable, and cost-effective communication framework. This transition marks a paradigm shift — from domain-specific and hierarchical networks to a **unified, service-oriented architecture,** laying the foundation for the **software-defined and autonomous vehicles** of the future.

3. Automotive Ethernet Fundamentals

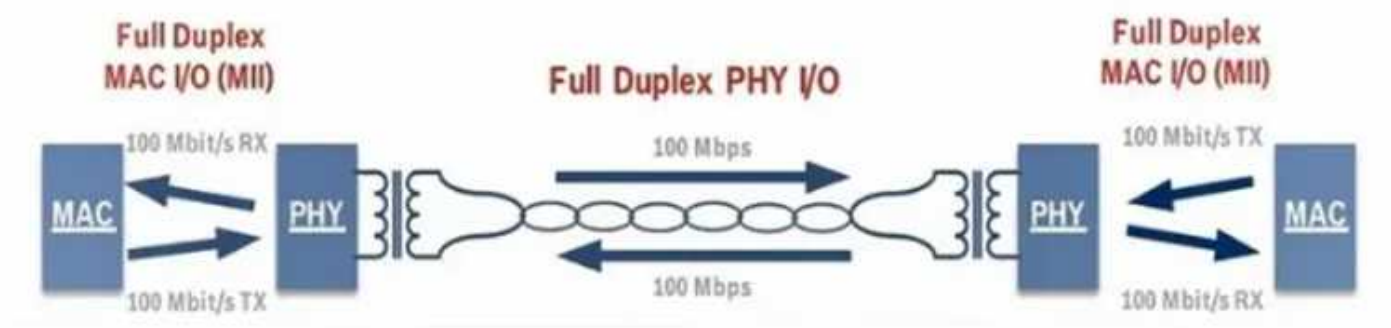
Automotive Ethernet is a specialized adaptation of conventional IEEE 802.3 Ethernet, engineered to meet the unique constraints and reliability requirements of in-vehicle environments. While it inherits Ethernet's packet-based communication model and layer structure, Automotive Ethernet extends it with modifications that address **determinism, electromagnetic compatibility (EMC), temperature resilience, and functional safety—**all of which are essential in automotive applications.

3.1 Physical Layer Innovations

Traditional Ethernet employs differential signaling over four or eight wire pairs, which is impractical for vehicles where weight, space, and EMI susceptibility are major concerns. Automotive Ethernet introduces Single-Pair Ethernet (SPE), which enables full-duplex communication over a single unshielded twisted pair (UTP) cable, significantly reducing wiring weight and cost.

Key physical layer standards include:

- **100BASE-T1 (IEEE 802.3bw):** 100 Mbps full-duplex communication over a single twisted pair up to 15 meters, used for body electronics and diagnostics.
- **1000BASE-T1 (IEEE 802.3bp):** 1 Gbps full-duplex operation for ADAS, camera, and sensor data aggregation.
- **10GBASE-T1 (IEEE 802.3ch):** 10 Gbps operation for backbone and zonal switch interconnections in high-performance computing domains.



These PHYs employ advanced modulation schemes such as PAM3 and PAM8 to achieve high data rates over lightweight cable, while maintaining stringent automotive-grade EMC performance.

3.2 Protocol Stack and Layer 2 Enhancements

Automotive Ethernet preserves the OSI layer model of traditional Ethernet but adapts its upper layers for in-vehicle determinism and time synchronization. The **Layer 2 (Data Link Layer)** serves as the foundation for traffic forwarding, frame filtering, VLAN tagging (IEEE 802.1Q), and multicast management—key functions handled by automotive Ethernet switches.
At higher layers, the use of **IP-based communication (IPv4/IPv6)** allows seamless integration with cloud and diagnostic networks, enabling over-the-air (OTA) updates and centralized vehicle management. Standard automotive middleware such as **SOME/IP (Scalable Service-Oriented Middleware over IP) and DoIP (Diagnostics over IP)** leverage Ethernet to establish service-oriented communication among ECUs.

3.3 Deterministic Communication through TSN

While conventional Ethernet operates on a best-effort delivery model, automotive applications require bounded latency and guaranteed message delivery for safety-critical systems. This is achieved through **Time-Sensitive Networking (TSN)** a set of IEEE 802.1 standards (including 802.1Qbv, 802.1AS, and 802.1Qbu) that define mechanisms for time synchronization, scheduled traffic, and frame preemption. TSN transforms Ethernet into a deterministic network capable of supporting real-time control and sensor fusion workloads alongside non-critical data streams.

3.4 Interoperability and Compliance

The automotive ecosystem enforces rigorous compliance and interoperability testing to ensure reliability across multi-vendor implementations. Organizations such as the **OPEN Alliance** define test specifications **(e.g., TC8 for interoperability)** that validate PHY behavior, frame forwarding, QoS handling, and TSN compliance under real-world conditions.
By combining standardized IEEE protocols with automotive-specific extensions, Automotive Ethernet provides the scalability, reliability, and interoperability required for next-generation vehicle networks—setting the stage for advanced switch architectures that can efficiently manage this complex communication landscape.

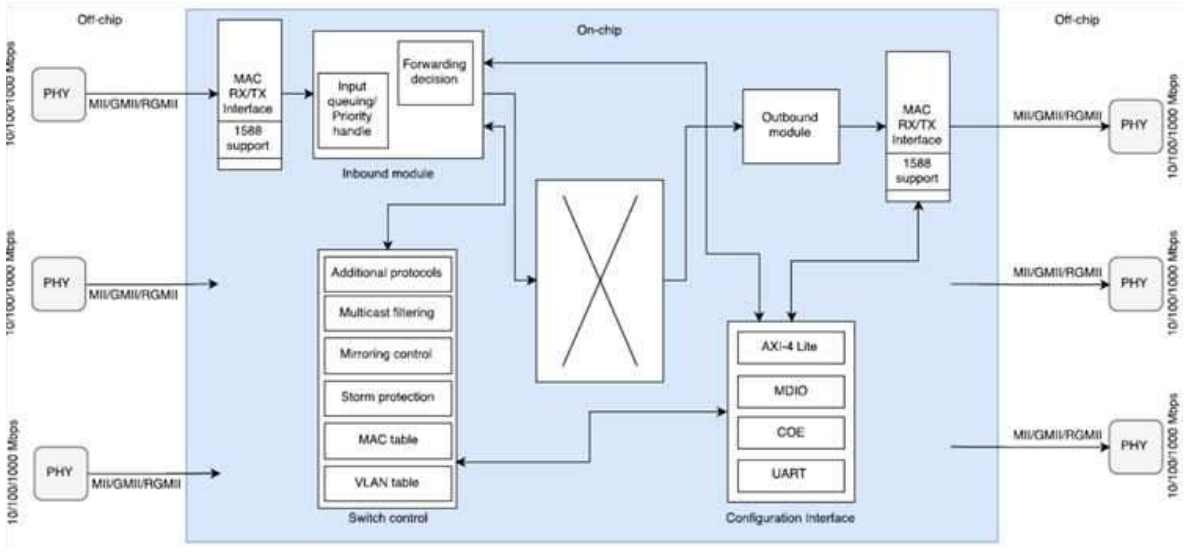
4. Role of the Automotive Ethernet Switch

As automotive networks transition from domain-specific architectures to **zonal and centralized topologies, the Ethernet switch** has become a critical component of the vehicle's communication backbone. The switch serves as the central node that interconnects Electronic Control Units (ECUs), sensors, and gateways across multiple domains, ensuring deterministic, high-bandwidth, and prioritized data delivery.

4.1 Switch Architecture Overview

An Automotive Ethernet switch operates primarily at the **Data Link Layer (Layer 2),** directing Ethernet frames based on MAC addresses and VLAN configurations. Modern switches integrate additional functions at higher layers to support **Quality of Service (QoS), Time-Sensitive Networking (TSN), and security policies.**

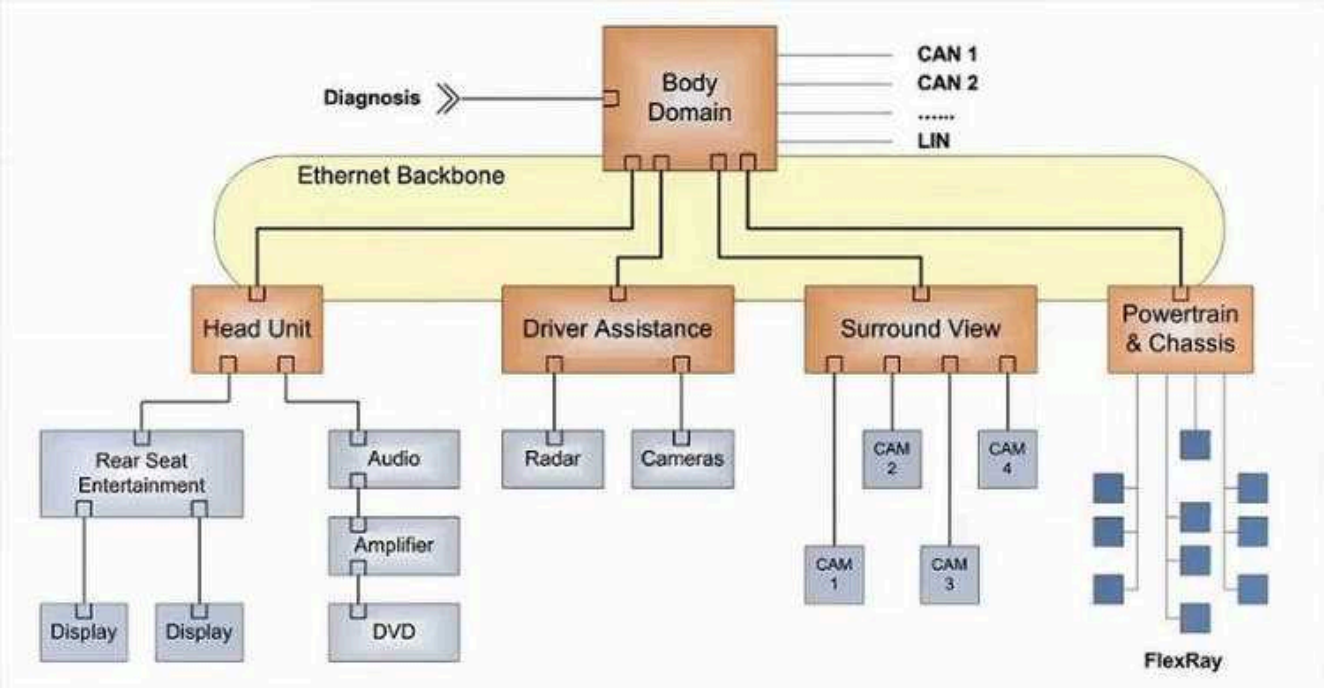
- **Ingress and Egress Ports:** Physical interfaces connected to ECUs or other switches.
- **Switch Fabric:** The internal high-speed matrix that determines how packets are forwarded.
- **Forwarding Engine:** Implements frame classification, MAC learning, VLAN tagging, and filtering logic.
- **QoS and TSN Scheduler:** Ensures that latency-sensitive traffic such as ADAS or control signals are prioritized.
- **Management and Control Plane:** Provides configuration interfaces through protocols like SNMP, NETCONF, or AUTOSAR Ethernet Stack.



Switches also include diagnostic and monitoring features to support in-vehicle testing, fault detection, and predictive maintenance.

4.2 Switches in Zonal and Centralized Architectures

Modern automotive switches integrate both **hardware-based forwarding and software-driven control logic.** Hardware acceleration ensures deterministic timing for TSN traffic, while microcontrollers enable dynamic configuration and diagnostics. Switch software stacks often align with **AUTOSAR Adaptive or POSIX-based RTOS** environments, allowing integration with higher-level orchestration systems and cloud-based management platforms. The below Zonal architecture has each functional component group ECUs by physical location (zone) — for example, Head Unit, Driver Assistance, Surround View and Powertrain ECUs connect them through regional switches to a **central Vehicle Body Domain compute.**



Automotive Ethernet switches in this setup:

- Aggregate sensor and actuator data within zones.
- Connect to backbone switches via Gigabit or **10 Gigabit links.**
- Enable efficient traffic routing between zones with minimal latency.
- Facilitate **service-oriented communication** using protocols such as SOME/IP and DDS.

This transition simplifies wiring harnesses, enhances scalability, and supports over-the-air (OTA) update frameworks through a unified Ethernet backbone.

4.3 Ethernet Switches Key Functions:

Automotive Ethernet switches perform several key functions tailored to automotive use cases:

- **Frame Forwarding and Filtering:** Switches learn MAC addresses dynamically and forward frames only to the appropriate ports, minimizing unnecessary traffic.
- **Virtual LAN (VLAN) Segmentation:** Logical separation of traffic domains (e.g., infotainment, ADAS, diagnostics) to improve security and network management.
- **Quality of Service (QoS):** Prioritizes traffic using IEEE 802.1p or DSCP marking to ensure deterministic latency for time-critical frames.
- **Time Synchronization:** Implements **IEEE 802.1AS (gPTP)** to provide nanosecond-level clock synchronization across ECUs, essential for sensor fusion and real-time control.
- **TSN Scheduling:** Supports standards like **802.1Qbv (Time-Aware Shaper)** and **802.1Qbu (Frame Preemption)** to guarantee transmission windows for high-priority data.
- **Security and Isolation**: Enforces MAC filtering, ingress policing, and DoS protection to safeguard the network from malicious or faulty nodes.

5. The Need for Ethernet in handling High-Bandwidth Automotive Data Streams

Today, CAN network supports a maximum data payload of **8 bytes per frame,** while CAN FD extends this to **64 bytes.** Although sufficient for controlling signals or diagnostics, this frame size is inadequate for continuous or bulk data transmission. For instance, transmitting a **500-byte dataset** over CAN FD requires.

- Over **60 frames,** each undergoing arbitration, transmission, and acknowledgment cycles.
- Corresponding **CPU overhead** for message fragmentation and reassembly.
- Increased **bus utilization** and **latency,** potentially impacting real-time control signals.

This fragmentation not only consumes significant processing resources but also complicates **message sequencing, timing analysis, and fault recovery,** making CAN unsuitable for high-throughput data paths.

5.1 Automotive Ethernet Data usage (Application)

Application	Typical Data Size per Message	Why Ethernet is Needed
Camera Data (ADAS / Surround View / Mirror Replacement)	~1–10 MB per frame	Raw or compressed video frames from multiple cameras (e.g., 720p @ 30fps) require Mbps to Gbps bandwidth — far beyond CAN (8 bytes/frame).
Radar / Lidar Sensor Streams	~1–5 kB per message	Sensor fusion data packets or raw point clouds are large; need low-latency, high-throughput Ethernet to transmit in real time.
Infotainment Streaming (Audio/ Video)	>1 MB per second	Media streams (e.g., between head units and rear seat entertainment) use IP-based audio/video (AVB/TSN) protocols over Ethernet.
Firmware Over-The-Air (FOTA) / Diagnostics over IP	~kB–MB range	When updating ECU firmware or transferring large diagnostic data, messages easily exceed 500 bytes. Ethernet enables faster ECU flashing.
High-Definition Map Updates (Navigation / Autonomous Driving)	MB–GB	Map and sensor fusion data exchanges with central compute nodes demand Ethernet-level bandwidth.
Vehicle-to-Everything (V2X) Gateway / Data Logging	~1–10 kB per message	Aggregated telematics data, event logs, and sensor data need efficient bulk transfer to gateways.
Centralized Zonal/ Domain Controllers	~kB–MB per transaction	Data consolidation from multiple ECUs (e.g., powertrain, chassis, ADAS) often exceeds CAN's 8-byte. payload limits.

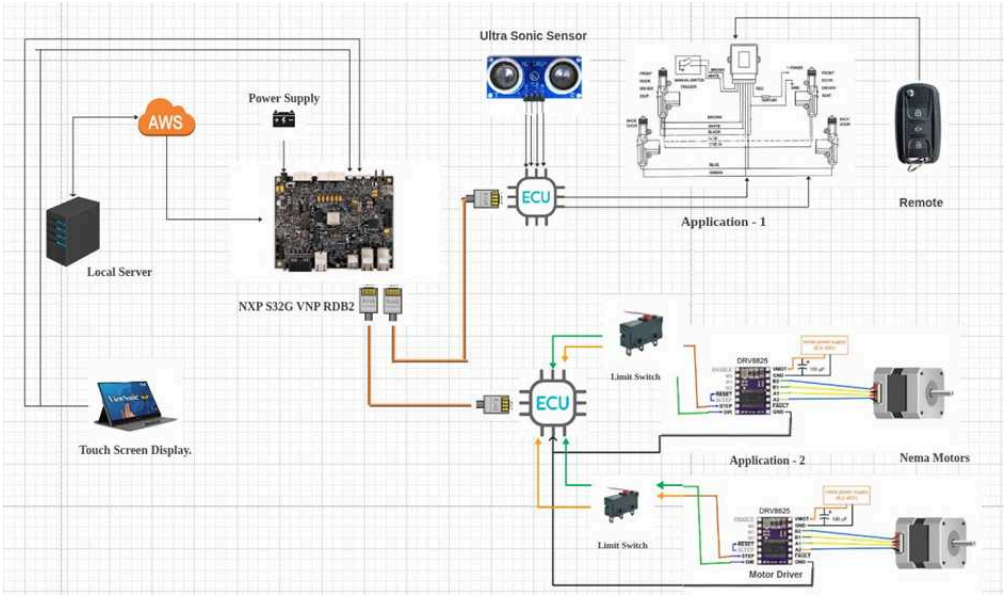
5.2 Automotive Ethernet vs CAN/ CAN FD Comparison

CAN and CAN FD remain valuable for low-bandwidth, real-time control functions, However the Automotive Ethernet has become important for modern vehicle data networks, due to its higher Max Transmission unit (MTU), scalable bandwidth, and time-sensitive capabilities, which provides robust foundation for sensor-rich, edge-compute, connected, and autonomous vehicles data streams. Migration to Automotive Ethernet is not merely a technological upgrade—it represents a fundamental architectural evolution that enables the future of intelligent mobility.

Feature	CAN	CAN FD	Ethernet
Max Payload	8 bytes	64 bytes	1500–9000 bytes
Data Rate	1 Mbps	2–8 Mbps	100 Mbps–10 Gbps
Transmission Type	Broadcast, Half Duplex	Broadcast, Half Duplex	Full Duplex
Determinism	High	High	High (with TSN)
Suitable For	Control, Diagnostics	Moderate Data (Sensors)	High Data (Video, Fusion, OTA)

6. Experimental Setup and Evaluation

The experimental platform is based on the NXP S32G-VNP-RDB2 automotive networking processor board, chosen for its high-performance Arm Cortex-A53 cores, integrated hardware security modules, and advanced Ethernet switching capabilities. The setup focuses on three core areas: secure firmware update, real-time Ethernet communication, and mixed-critical workload virtualization.



6.1. System Overview

The experimental setup demonstrates a secure **Over-the-Air (OTA)** firmware update mechanism for distributed automotive electronic control units (ECUs) using **AWS IoT Core** as the cloud service and an **Automotive Ethernet Switch** as the in-vehicle gateway. The two end applications under consideration are the **Sunroof Control System** and the **Door Lock Control System.** The Ethernet switch acts as an intelligent intermediary, receiving firmware updates from the cloud, validating their authenticity, and forwarding them to the respective end devices based on predefined metadata and routing logic.
This experiment emulates a real-world automotive environment where multiple ECUs coexist under a centralized in-vehicle gateway, enabling secure, efficient, and reliable firmware distribution.

6.2. System Topology

The overall topology consists of three major layers:

1. **Cloud Layer (AWS IoT Core)**
2. **Gateway Layer (Automotive Ethernet Switch)**
3. **End Application Layer (Sunroof ECU and Door Lock ECU)**

6.3. Functional Description

6.3.1 AWS IoT Core

AWS IoT Core functions as the **centralized OTA management platform.** It hosts and maintains version-controlled firmware binaries for both the Sunroof and Door Lock ECUs. Firmware images are digitally signed with public key infrastructure (PKI) for authenticity and integrity. When new firmware release is ready, AWS IoT Core publishes an OTA job specifying metadata such as:

- Target device group (e.g., “Sunroof” or “Door Lock”)
- Firmware version number
- Hash and signature for validation.
- Download URL or MQTT topic reference.

The job is sent securely to the Automotive Switch via **MQTT over TLS,** protecting it from tampering and keeping it confidential.

6.3.2 Automotive Ethernet Switch

The Automotive Ethernet Switch serves as the local OTA orchestrator within the vehicle network. It performs the following key functions:

1. **Firmware Reception:**
   Receives OTA job notifications and firmware binaries from AWS IoT Core via the secure channel.
2. **Authentication and Verification:**
   Validates the firmware's digital signature using pre-stored public keys to confirm the source of authenticity.
3. **Decision Logic:**
   Parses the firmware metadata to identify the target ECU (Sunroof/or Door Lock). Based on this, the switch determines the appropriate transmission path.
4. **Firmware Distribution:**
   Forwards the validated firmware image to the designated ECU using **Ethernet-based communication protocols** such as **Diagnostics over IP (DoIP)** or a custom TCP-based transport channel.
5. **Update Monitoring and Reporting:**
   Collects update status from each ECU and reports the consolidated result (success, failure, or rollback) back to AWS IoT Core.

This layer effectively acts as a **secure and intelligent firmware router,** preventing the need for each ECU to individually connect to the cloud.

6.3.3 End Application ECUs

Each end ECU incorporates a lightweight bootloader with the following capabilities:

- Receive firmware packets from the switch over Ethernet.
- Validate digital signature and checksum before flashing.
- Perform secure firmware updates with rollback protection in case of verification failure.
- Acknowledge the switch after completion.

The Sunroof ECU and Door Lock ECU thus represent independent end devices capable of self-verification and secure firmware management.

6.4. Communication and Security Mechanisms

Layer	Protocol / Mechanism	Purpose
Cloud ⟷ Switch	MQTT / HTTPS over TLS 1.2	Secure OTA job delivery and firmware download
Firmware Package	RSA / ECDSA Digital Signature	Ensures firmware integrity and authenticity
Switch ⟷ ECUs	DoIP / TCP over Ethernet	Reliable in-vehicle firmware transfer
Bootloader	Secure Boot with Rollback Prevention	Guarantees only trusted firmware executes

6.5. Experimental Evaluation

OTA firmware updates were sent from AWS IoT Core to both ECUs using the Ethernet Switch. The switch correctly identified the firmware target based on metadata and routed the respective images to the appropriate ECU.
Key performance metrics observed:

- **Update Time:** Gateway distribution lowered download latency by retrieving firmware from the cloud once and distributing it locally.
- **Security Validation:** Firmware signature verification succeeded in all test runs, ensuring integrity protection.
- **Reliability:** In cases of simulated failure (e.g. A checksum mismatch triggered rollback mechanisms, highlighting the design's effectiveness.

This experiment validated that the proposed topology provides secure, scalable, and efficient OTA architecture for connected automotive systems.

7. Conclusion

Automotive Ethernet has become the cornerstone of next-generation in-vehicle networks, delivering high bandwidth, scalability, and interoperability. By replacing legacy, domain-specific communication buses with a unified Ethernet backbone, automakers are adopting advanced design paradigms such as zonal architectures, software-defined vehicles (SDV), and centralized computing. The Ethernet switch plays a pivotal role in this transformation, acting as the intelligent interconnect that links sensors, actuators, and compute platforms with deterministic precision and strong security. As vehicles become increasingly data-driven, managing switch configurations, firmware updates, and real-time data flows has grown more complex. In this environment, test automation has evolved from a productivity tool into a critical assurance mechanism. Using Python-based automation frameworks, engineers can efficiently validate Layer 2 functionalities, TSN compliance, and QoS behavior, ensuring reliable performance under diverse traffic and environmental conditions. Automation further enables continuous validation through CI/CD pipelines, aligning with the fast iteration cycles of modern automotive software.

8. Future Scope

The convergence of **Ethernet, AI, and automation** will shape the future of in-vehicle networking. Emerging capabilities such as predictive testing, self-healing diagnostics, and virtualized test environments will drive faster innovation while ensuring safety and compliance. With continued advancements led by **IEEE and the OPEN Alliance,** Automotive Ethernet is moving toward **multi-gigabit, low-latency, and energy-efficient** network architectures—forming the digital nervous system of autonomous and connected vehicles.

The combination of **Automotive Ethernet and intelligent automation** enables scalable, secure, and advanced automotive networks. As vehicles transition toward autonomy and cloud integration, Ethernet-based infrastructures supported by robust automated testing will remain fundamental to delivering safety, reliability, and innovation.

TESSOLVE
A HERO ELECTRONIX VENTURE

Reference

1. https://semiengineering.com/knowledge_centers/automotive/automotive-networking/automotive-ethernet-time-sensitive-networking-tsn/
2. https://www.ti.com/product-category/interface/ethernet-ics/ethernet-phys/overview.html
3. https://intrepidcs.com/products/automotive-ethernet-tools/automotive-ethernet-switch/
4. https://www.prodigytechno.com/difference-between-lin-can-and-flexray-protocols
5. https://www.technica-engineering.com/extreme-networking-switch-2/
6. "Ethernet switching-the enabling technology of SOHO implementation" by D. H. Chung – IEEE.
7. "Comparative Analysis of CAN-FD and 10BASE-T1S Ethernet for Time-Critical Applications in Automotive Networks" by C. Hein, K. Matheus, and J. Berlak – IEEE.
8. "Performance Analysis of IEEE 802.1Qch for Automotive Networks: Compared with IEEE 802.1 Qbv" by B. Wang, F. Luo, and Z. Fang – IEEE.

Author
Anand Srinivasavarathan
Software Engineer 1,
Semicon Automotive

Co-Author
Dhanendran Narayanan
Associate Director,
Semicon Automotive

About Tessolve

Technology drives Tessolve's role as a premier end-to-end silicon and systems partner. With over 3,000 employees across 10 countries and a robust 20+ year history, Tessolve has delivered substantial impact through its advanced labs and innovative solutions.

Connect With Us

sales@tessolve.com

www.tessolve.com

India | USA | Singapore | Malaysia | Germany | United Kingdom | Japan | Taiwan | Philippines | Canada | Netherlands