International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 7 Issue 4, July-August 2023 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Connected Vehicles, Zonal In-Vehicle Network Architecture

Sanath D Javagal

Senior, AV Network Systems Engineer, Autonomous Vehicle Industry, United States

ABSTRACT

In-vehicle network architecture is crucial in modern automobiles, enabling the seamless integration of electronic components and systems within vehicles. This article provides an in-depth exploration of in-vehicle network architecture, covering its history, types of networks, communication protocols, and emerging trends. The history section highlights the development of in-vehicle networks, from basic electrical systems to the introduction of standardized protocols like the Controller Area Network (CAN). The types of networks section discusses Local Interconnect Network (LIN), CAN, and Automotive Ethernet, outlining their characteristics and applications. The communication protocols section explores protocols such as CAN, LIN, FlexRay, MOST, and Ethernet, detailing their features and use cases. Additionally, the article delves into emerging trends, including connected vehicles, advanced driver assistance systems (ADAS), autonomous vehicles, and cybersecurity. The discussion emphasizes the increasing need for high-bandwidth, low-latency communication and robust cybersecurity measures in modern vehicles. By understanding in-vehicle network architecture and its evolving landscape, automotive engineers and stakeholders can navigate the complexities of designing advanced, connected vehicles that ensure safety, efficiency, and a superior driving experience.

KEYWORDS: *Vehicle Network Architecture, Connected Vehicles, Zonal Architecture, Automotive Network, Advanced Driver Assistance Systems, Cybersecurity*

How to cite this paper: Sanath D Javagal "Connected Vehicles, Zonal In-Vehicle Network Architecture" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-7 | Issue-4, August 2023, pp.81-85, URL: www.ijtsrd.com/papers/ijtsrd59616.pdf

IJTSRD59616

INTRODUCTION

In-vehicle network architecture is an essential aspect of modern automobiles. It refers to the complex system of interconnected electronic components within a vehicle that enables various functionalities, such as engine control, infotainment systems, and driver assistance features. As the complexity of vehicles continues to increase, so does the need for more advanced in-vehicle network architecture to manage the increasing number of electronic components and systems.

This paper aims to thoroughly explain in-vehicle network architecture, including its history, types of networks, communication protocols, and emerging trends.

History of In-Vehicle Network Architecture

The use of electronic components in vehicles dates back to the 1960s, when basic electrical systems, such as engine control and lighting, were introduced. However, it was in the 1980s that in-vehicle network architecture began to take shape. In the early 1980s, General Motors (GM) introduced the first electronic engine control system, which used a simple data bus to connect various engine control components.

The first standardized in-vehicle network architecture was introduced in the early 1990s when Robert Bosch GmbH developed the CAN (Controller Area Network) protocol. The CAN system was created specifically for the automotive industry and enables electronic components to exchange messages through a common bus. Network protocol enabled the development more sophisticated electronic systems, such as anti-lock braking systems and electronic stability control.

Today, in-vehicle network architecture has evolved significantly, with modern vehicles containing numerous electronic components and systems that

require complex communication and control. This section will give you an overview of the current types of in-vehicle networks being used.

Zonal In-Vehicle Network Architecture

Zonal vehicle network architecture is a technical framework that organizes the electronic systems and components within a vehicle into separate zones, each responsible for specific functionalities. It aims to enhance the modularity, scalability, and flexibility of the vehicle's network infrastructure while improving overall system performance and reducing complexity.

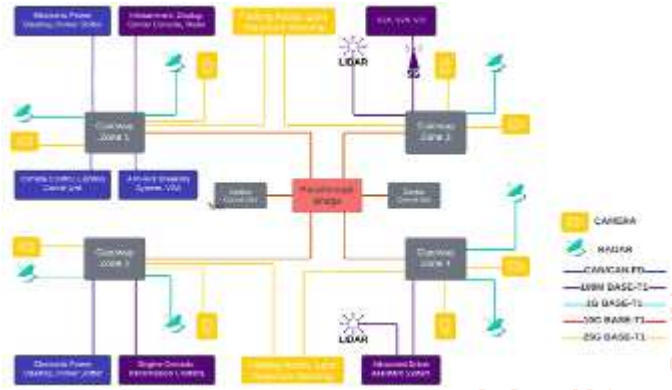

Figure 1 An example of a zonal in-vehicle network architecture

1. Zonal Structure: The vehicle is usually partitioned into different zones based on its functions, like powertrain control units, chassis control units, body control units, and infotainment control units. These zones have electronic control units (ECUs) that manage various subsystems.
2. Zone Controllers: Each zone is equipped with a zone controller, which acts as a central hub for the ECUs within that zone. The zone controller provides connectivity, communication, and coordination between the ECUs, enabling them to work together seamlessly. It also handles data exchange between the zones.
3. Ethernet Backbone: Zonal architectures often utilize an Ethernet-based backbone network, which serves as the primary communication infrastructure within the vehicle. Ethernet offers high bandwidth, low latency, and scalability, making it suitable for handling the increasing data demands of modern vehicle systems.
4. Gateway Units: Gateway units are responsible for interconnecting the different zones within the vehicle. They manage communication between the zone controllers and facilitate data exchange across zones, allowing information to flow between subsystems.
5. Distributed Intelligence: Zonal architectures promote the concept of distributed intelligence, where decision-making and processing capabilities are distributed across the various ECUs within each zone. This approach reduces the reliance on a single centralized controller, improving fault tolerance and enabling faster response times.
6. Standardized Protocols: Zonal architectures often rely on standardized communication protocols to ensure interoperability and compatibility between components and subsystems. Protocols like CAN, and Automotive Ethernet (e.g., BroadR-Reach, 1000BASE-T1, 10GBASE-T1) are commonly used for intra-zone and inter-zone communication.
7. Scalability and Flexibility: Zonal architectures provide scalability by including or excluding entire zones or individual ECUs per the vehicle's requirements. This flexibility simplifies system integration, facilitates future upgrades, and supports modular vehicle designs.
8. Security and Safety: Zonal vehicle networks incorporate security measures to protect against unauthorized access and potential cyber threats. Additionally, safety considerations are essential to ensure that vital systems, like braking and steering, remain isolated from less critical functions to prevent any compromise in vehicle safety.

Overall, zonal vehicle network architecture optimizes integrating various electronic systems within a vehicle by organizing them into zones and leveraging standardized communication protocols. It enhances modularity, scalability, flexibility, and system performance while maintaining security and safety standards.

Communication Protocols

Various communication protocols enable electronic components to interface with other components and the types of in-vehicle networks. The main communication protocols used in In-vehicle network architecture are:

1. Controller Area Network (CAN): In in-vehicle network architecture, the CAN communication protocol is used most. A message-based protocol allows electronic components to exchange data in real time. CAN operate using two types of messages: data frames and remote frames.

Data frames are used to transmit actual data, while remote frames are used to request data from another electronic component. CAN also support fault tolerance, which means that if one component fails, the rest of the network can still operate.

2. Local Interconnect Network (LIN): LIN is a single-wire communication protocol primarily

used for low-bandwidth applications. It is a master-slave protocol, meaning a master electronic component controls communication with several slave components.

LIN is often used in interior lighting, door locks, and window controls. It is unsuitable for high-bandwidth applications because of its low speed and limited capabilities.

3. FlexRay: FlexRay is a high-speed communication protocol developed for advanced automotive applications like steer-by-wire and brake-by-wire systems. It operates at up to 10 Mbps speed and supports time-triggered and event-triggered communication.

FlexRay also supports fault tolerance and redundancy, making it a reliable protocol for critical automotive applications. It is less widely used than CAN or Ethernet but is becoming increasingly popular in high-end vehicles.

4. Media-Oriented Systems Transport (MOST): MOST is a multimedia transmission protocol for in-vehicle infotainment systems. It operates at up to 150 Mbps speed and supports audio, video, and data transmission.

MOST is a multi-master protocol, which means that multiple electronic components can control communication on the network. It also supports fault tolerance and redundancy, making it a reliable protocol for in-vehicle multimedia systems.

5. Ethernet: Ethernet is a high-speed communication protocol becoming increasingly popular in in-vehicle network architecture. It operates at up to 25Gbps speed and supports data, audio, and video transmission.

Ethernet uses the IP protocol, which enables seamless integration with other devices and networks. It also reinforces Quality of Service (QoS) to prioritize traffic and ensure that critical data is transmitted with minimal delay.

Emerging Trends in In-Vehicle Network Architecture

As in-vehicle technology evolves, several emerging trends are shaping the future of in-vehicle network architecture. The most significant trends are:

1. Connected Vehicles: The automotive industry is witnessing a rise in the use of connected vehicles. These vehicles are equipped with wireless communication technology, including Wi-Fi and cellular networks, allowing them to connect to the internet and other devices.

Connected vehicles can interface with other vehicles, infrastructure, and devices, improving safety, traffic flow, and the overall driving experience. In-vehicle network architecture will play a critical role in enabling this connectivity and facilitating communication between the various components of connected vehicles.

2. (ADAS) Advanced Drive Assistance System: ADAS refers to a collection of electronic systems that aid drivers in operating their vehicles. These systems rely on different sensors, cameras, and other electronic components to continuously monitor the surrounding environment and offer immediate feedback to the driver.

ADAS systems are becoming increasingly common in modern vehicles and are looking forward to playing a significant role in the future of automotive technology. In-vehicle network architecture will need to support the high-bandwidth communication and processing required by these advanced systems.

3. Autonomous Vehicles: Autonomous/Self-Driving vehicles are vehicles capable of functioning without human intervention. They use a combination of sensors, cameras, and other electronic components to navigate and operate safely on the road.

In-vehicle network architecture will be critical for the operation of autonomous vehicles, as it will enable communication between the various electronic components and systems required for autonomous operation.

Autonomous vehicles will require high-bandwidth, low-latency communication to ensure timely and accurate data exchange between components. In-vehicle network architecture will need to support this level of communication to enable safe and reliable autonomous operation.

4. Cybersecurity: Cybersecurity will become a critical concern as vehicles become more connected and rely more heavily on electronic systems. There is a risk of unauthorized access and potential harm caused by hackers and malicious individuals exploiting vulnerabilities in the vehicle's network architecture. If not addressed, there is a risk of compromised sensitive information and even the possibility of the vehicle being controlled by unauthorized individuals.

The network architecture of vehicles needs to have strong cybersecurity measures in place to avoid any unauthorized access and guarantee the safe and trustworthy functioning of the vehicles. These

security measures can consist of things like encryption, secure authentication, and intrusion detection systems.

Connectivity in Connected Vehicles

Connected vehicles leverage various types of connectivity, both within the vehicle and with the external environment. They are interconnected through V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure), V2N (Vehicle-to-Network), and V2X (Vehicle-to-Everything) communications.

1. Vehicle-to-Vehicle (V2V): With V2V communication, vehicles can exchange vital information like their speed and location, effectively decrease the chances of accidents and improving road safety.
2. Vehicle-to-Infrastructure (V2I): With V2I communication, vehicles can interact with traffic infrastructure such as traffic signals, road signs, and traffic management systems. This enables smoother and more efficient traffic flow.
3. Vehicle-to-Network (V2N): In V2N communication, information is exchanged by connecting a vehicle CPU and the telecommunication network. This allows the vehicle to access cloud-based services such as real-time traffic information and remote diagnostics.
4. Vehicle-to-Everything (V2X): V2X communication is the ultimate form of communication, enabling a vehicle to connect with every entity that could have an impact on it or be impacted by it. V2X includes other vehicles, infrastructure, pedestrians, and network.

Future of Connected Vehicles: 5G and Beyond

The advent of 5G is set to revolutionize the connected vehicle space. With its ultra-low latency, high data rates, and the ability to connect many devices, 5G will unlock the true potential of connected vehicles, supporting real-time V2X communications and enabling advanced features such as remote vehicle control and autonomous driving. Furthermore, 6G, envisioned to provide even higher data rates and lower latency than 5G, is expected to push the boundaries of connected vehicles further.

Conclusion

The future of transportation is undeniably connected and intelligent, and advances in in-vehicle network architecture and communication technologies are shaping this future. With the increasing connectivity of vehicles, the in-vehicle network architecture will need to evolve to support higher data rates, increased safety, and more advanced functionalities, paving the way for an era of safe, efficient, and intelligent mobility.

In-vehicle network architecture is a critical aspect of modern automobiles. It enables the various electronic components and systems within a vehicle to communicate and operate effectively, supporting various functions like engine control systems, infotainment systems, and driver assistance features.

In-vehicle network architecture has evolved significantly since its inception in the 1980s, with standardized protocols like CAN and the recent development of high-speed Ethernet networks. As in-vehicle network technology advances, emerging trends such as connected vehicles, ADAS, and autonomous vehicles will shape the future of in-vehicle network architecture.

The architecture of in-vehicle networks must accommodate the high-bandwidth and low-latency communication that advanced systems require. It must also incorporate strong cybersecurity measures to guarantee vehicles'. As automotive and transportation technology evolves, the in-vehicle network architecture will become increasingly crucial in enabling the next wave of advanced vehicles.

References

[1] Bosch, R. (1991). The CAN bus: From theory to practice. SAE Technical Paper 911605. doi:10.4271/911605

[2] Karsai, G., Neugschwandtner, G., & Pagany, Z. (2005). In-vehicle network technologies for next-generation cars. IEEE Transactions on Industrial Electronics, 52(4), 1016-1025. doi:10.1109/TIE.2005.852922

[3] Zhang, X., Sun, Y., & Jiang, Y. (2017). In-vehicle network: A review and future trends. IEEE Access, 5, 1867-1887. doi:10.1109/ACCESS.2017.2651199

[4] Gmach, D., Scholl, G., & Thiele, L. (2007). Design considerations for FlexRay-based in-vehicle networks. IEEE Transactions on Industrial Informatics, 3(3), 226-239. doi:10.1109/TII.2007.903297

[5] Weisenburger, T., & Wolf, L. (2013). Automotive Ethernet – The definitive guide. Springer.

[6] Hoyer, V., & Taha, A. (2015). Ethernet for in-vehicle networking: A survey. IEEE Communications Surveys & Tutorials, 17(3), 1778-1796. doi:10.1109/COMST.2015.2394296

[7] Chatterjee, M., Shukla, A., & Shin, K. G. (2019). Security and privacy for in-vehicle networks: Challenges and opportunities.

[8] IEEE Communications Surveys & Tutorials, 21(4), 3717-3742. doi:10.1109/COMST.2019.2920604

[9] Guo, H., Zhang, M., & Riaz, R. A. (2020). Connected vehicles: Intelligent transportation system for smart cities. In IoT for smart cities: technologies, big data, and security (pp. 169-199). Springer, Cham.

[10] A. Elzanaty, M., Sukuvaara, T., & Sutinen, T. (2019). The high-level design of modern in-vehicle architecture using ethernet and controller area network (CAN). IEEE Access, 7, 148270-148281.

[11] Zeadally, S., Siddiqui, F., & Baicher, G. S. (2020). Connected vehicles: Solutions and challenges. IEEE Internet of Things Journal, 7(7), 5925-5942.

[12] M. R. Palattella et al. (2016). Internet of Things in the 5G Era: Enablers, Architecture, and Business Models. IEEE Journal on Selected Areas in Communications, 34(3), 510-527.