Important Role of Ethernet Switches in Vehicles E/E Architectures

AVNET SILICA

MARVELL

Avnet Silica partners with Marvell to help develop cutting-edge customer solutions using the latest Ethernet Technologies.

INTRODUCTION

The quantity of electronics content found in a modern car is quite staggering. Back in the 1990s there would have only been a relatively small number of electronic controls units (ECUs) taking care of a few key tasks. With the advent of advanced driver assistance system (ADAS) technology and the integration of increasingly more sophisticated in-vehicle infotainment (IVI) features, things are proving to be very different today. Now even an economy level car can possess as many as 100 distinct ECUs, while a luxury model might have in excess of 150.

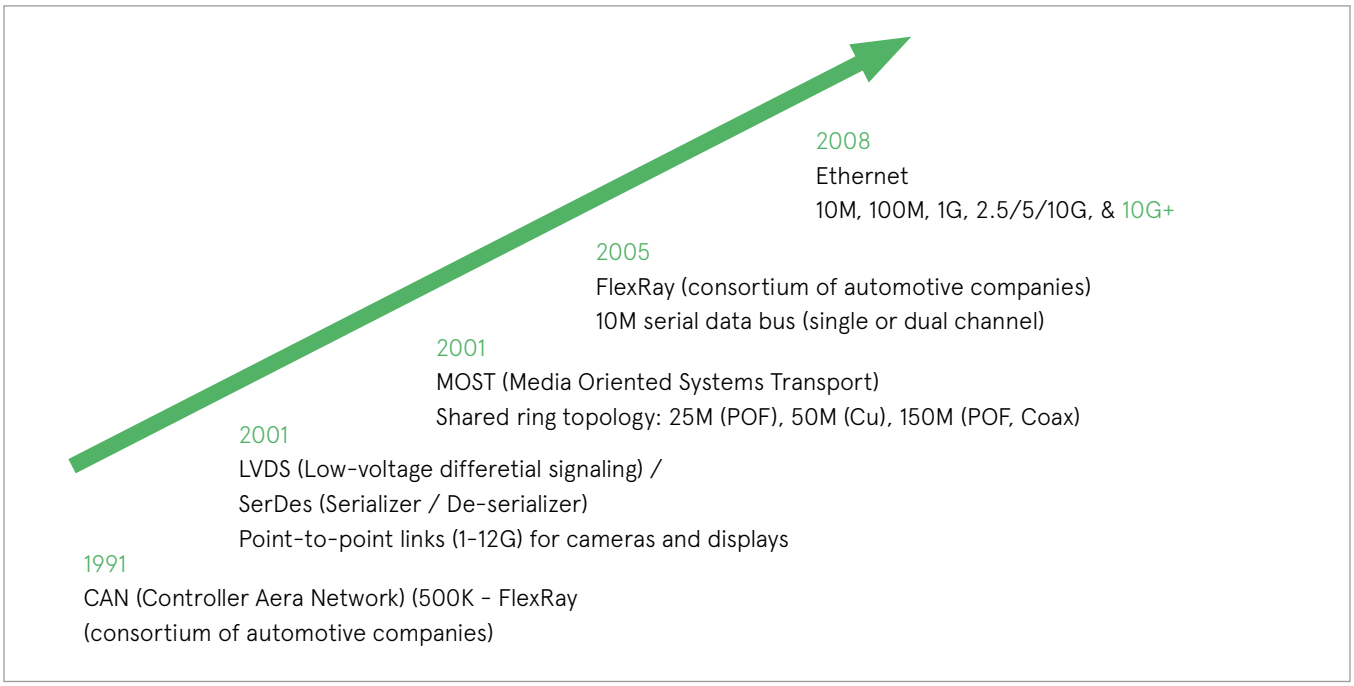

Figure 1: Automotive Networking Evolution

SCALABILITY

We have now reached a stage where nobody really doubts that it will be Ethernet that forms the foundation of in-vehicle networking infrastructure in the future. It is already superseding the long-established protocols, like CAN, which have almost reached the end of their usefulness as data rates continue to ramp up unrelentingly. This technology offers a variety of different attractive attributes. In particular, it presents a way of circumventing the serious bandwidth bottlenecks that incumbent protocols are starting to pose - delivering a long-term scalable networking platform with the capacity to support a plethora of more data-intensive applications as they are introduced over the course of the next few years to support the industry's push towards autonomous driving platforms. HD imaging and LiDAR are among the functions that will become commonplace thanks to automotive Ethernet rollout, enabling higher degrees of safety to be witnessed. Though automobile manufacturers are driving forward with the widespread deployment of Ethernet-based technology in their next generation models, they need to be confident that the security aspect has been comprehensively dealt with, as they simply cannot afford to generate bad press in what is such a competitive market.

The automotive business is one that relies heavily on reputation. Because legacy networks were not originally developed with security in mind, car manufacturers are keen to move to a network technology that is more resilient to potential attacks. However, before fully committing to Ethernet, they must be totally convinced that the constituent semiconductor technology has all the necessary protective measures in place to prevent vehicle occupants (as well as other road users) from coming to any harm.

What differentiates automotive Ethernet from normal Ethernet technology is that the time-critical nature of many of the functions it will support means that determinism is required. If there were latency issues of some kind that resulted in data packets being transported from a sensor module to an electronic control unit (ECU), for example, were delayed, then the ECU may not have enough time to react and a situation might arise where lives are put at risk. Mechanisms therefore need to be implemented which ensure that deterministic operation is continuously maintained.

ETHERNET FOR THE AUTOMOTIVE SECTOR

In 2015, the IEEE made the automotive 100Mbps single twisted pair Ethernet an international standard with the 802.3bw specification. In the following year, the IEEE then completed the approval of the 802.3bp Ethernet specification, which enables automotive connectivity at 1Gbps data rates, also over single twisted pair wires. What sets the automotive Ethernet standards apart from enterprise and consumer Ethernet standards is the fact that these speeds are now attainable on just one pair of wires as opposed to the conventional four pairs of wires. Because of needs for even higher speeds, the IEEE is now actively developing future Ethernet specifications that will allow for even greater speeds. The goal of these future standards is also to attain these speeds using the lightest and cheapest kind of cabling.

IMPORTANCE OF SWITCHES

As feature content increase the need for more bandwidth increases and the Switch then becomes a crucial component that connects ECUs on Ethernet at multiple speeds from 10Mbps to MultiGig. The Switch then becomes the crucial component to provide the means to exchange, route and share the data between Sensors/Actuators and ECUs. The Switch becomes the de facto component that enables the ability to transport and route data between a variety of Ethernets speeds as they will share a common set of IP/Protocols.

SECURITY

Security will become a crucial issue, and this can be better controlled from a component that is at the heart of the E/E Architecture rather than one distributed in many ECUs.

The huge prevalence of Ethernet technology does mean that, in theory, there are a greater number of potential hackers out there who could look to breach a vehicle's network security. Hackers can try to access the in-vehicle network via the LTE mobile connections, Wi-Fi or Bluetooth, by physically plugging into an Ethernet diagnostics ports in the vehicle, or by other means. By application of deep packet inspection (DPI), employing ternary content-addressable memory (TCAM), which is already commonly used in datacenter applications, in-depth investigation of each packet can be carried out. Through this it is possible to determine if the Ethernet packets entering the network belong within the vehicle or not, without latency rising or any extra software burden manifesting itself. Ethernet switches are also highly configurable devices, so it is of utmost importance to make it impossible for hackers to gain access to the switch to change network, filtering, and/or security parameters.

FUNCTIONAL SAFETY

TThe trend of moving mechanical elements from vehicles designs (to allow weight savings) has already meant that critical functions are dependent on the in-vehicle networking. Brake-by-wire and steer-by-wire have started this process and over time the semi-/fully autonomous functions already described will be added. Functional safety will thus become

an increasingly important aspect of automobile construction, with built-in redundancy and self-healing networks being needed to ensure the well-being of vehicle occupants (and other road users). More forward-thinking IC vendors, such as Marvell, are now recognizing that functional safety needs to be addressed right down at the silicon level. As a result, the company is addressing the needs of ASIL A/B/C all the way to ASIL D (the highest level of functional safety) - which will be encompassed within its future generations of Ethernet switches.

Figure 2: Marvell's 88Q5050 Automotive Gigabit Ethernet Switch

We are not far from reaching the point when Ethernet will soon become the primary and dominant in-vehicle networking protocol. It offers the scalability needed to attend to increasing data capacity requirements as they start to emerge, with headroom to deal with multi-Gigabit operation when this becomes necessary. Automotive manufacturers and their tier 1 systems integrators will thus be provided with a truly future-proof technology.

Currently many of the Ethernet switch ICs targeted at in-vehicle networking are simply consumer or industrial Ethernet switches that have been modified for this purpose. What is needed instead is optimized solutions that have been built from the ground up for automotive deployment. The Marvell 88Q5050 is an AEC-Q100-qualified 8-port SoC that is the first to actually support the 1Gbps automotive Ethernet data rates outlined by the 802.3bp standard. The IC also has a wealth of key security facets. Its trusted boot authentication functionality ensures that the software being used is correct before initiating booting-up. The embedded hardware DPI engine utilizes TCAM to inspect all packets coming in from all ports at the same time. Based on the programmed settings of the DPI engine, it can then determine the appropriate action for each packet on an individual basis. The switch IC can work out what action needs to be taken without having to call for additional support from the system processor resource (meaning that additional time is not taken up, latency is not effected, and the central processing unit can focus on other important tasks). Blacklisting and whitelisting of source and destination addresses further safeguard against the possibility of security breaches taking place.

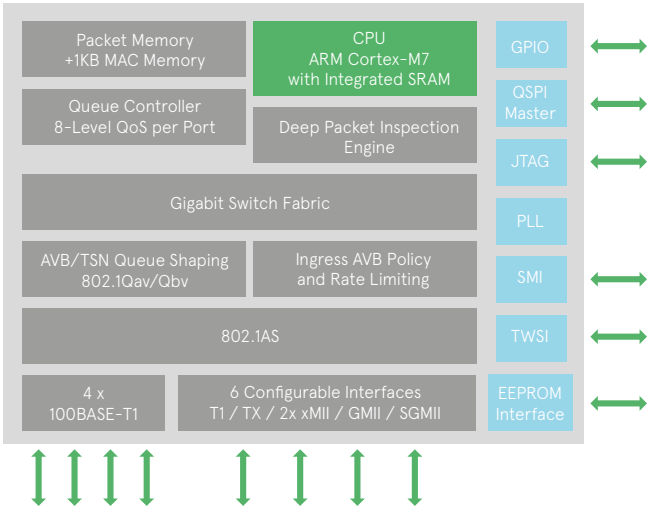

Figure 3: Functional Block Diagram for 88Q5050

CONCLUSION

In conclusion, current in-vehicle networking protocols are reaching the end of their usefulness in next generation architectures, as the data transfer levels in cars continue to escalate. Ethernet and Ethernet Switches and their attributes will enable car manufacturers to bring next generation vehicles to market - in terms of performance, flexibility and scalability. The wholesale implementation of Ethernet connectivity into automobiles is now well underway. This will allow car manufacturers to realize an array of different key operational benefits. As well as accommodating the elevated data rates that are now being envisaged, it will allow wire harnessing to become more lightweight and simpler - thereby resulting in reduced cost and improved performance. Though basic LiDAR systems may rely on single Gigabit networks, as more sophisticated systems with higher resolutions are deployed, then greater data capacity will be mandated. Likewise, it is expected that as the levels of autonomy increase there will be a need for the transfer of uncompressed imaging data - so that image quality is not degraded or latency added. This means that multi-Gigabit is not going to be that far away - with the IEEE already working on defining a 10Gbps automotive Ethernet standard.

By Hari Parmar, Principal Automotive System Architect, Marvell

By Thomas Foj and Gregor Knappik, Avnet Silica