White Paper

Testing Automotive Ethernet PHY

Critical New Test Challenges Facing Developers of Connected Vehicles

Introduction

Ethernet has long been the standard for data communication across local area networks (LANs), with the result that today's IT and telecommunications professionals are well versed in the unique challenges of testing Ethernet/IP performance.

But Ethernet is a relatively new proposition for automotive OEMs. Offering significant cost and performance benefits over legacy in-vehicle networking technologies, it is set to play a growing role in future in-vehicle networks—and it now has a viable PHYsical layer standard for the automotive industry, in the form of OPEN Alliance 100BASE-T1/ 1000BASE-T1 specifications.

There is little doubt that the next few years will see significant sustained growth in the extent and importance of Ethernet networking in vehicles. The industry is converging upon 100BASE-T1/1000BASE-T1 as its preferred PHYsical standard, and the **benefits of 2-wire Ethernet** cabling over conventional technologies are simply too great to ignore. (See page 3.)

However, the arrival of new systems and protocols requires **new testing approaches**, and will increase demands upon automotive research and development engineers in terms of network expertise. (See pages 3-4.)

What's more, Ethernet also presents the automotive industry with an entirely new challenge that, unless taken seriously, could prove catastrophic for safety, reliability and brand reputation: **network security**.

Potentially, making Ethernet the backbone of a car's network exposes critical performance and safety systems to the risk of attack—bringing automotive into the frontline of the rapidly evolving world of IT security. (See page 5.)

This white paper aims to give managers, team leaders—indeed anyone with a responsibility for ensuring the quality of the next-generation of vehicles—a high-level, functional overview of the key issues involved.

As a member of the OPEN Alliance SIG, Spirent's network testing engineers have been working closely with the industry to develop tailored answers to the challenges the emerging technologies bring, ensuring tomorrow's vehicles take full advantage of the many benefits of Automotive Ethernet.

The Evolution of Automotive Networking

To date, the varying operational requirements of different electronic functions have led automotive manufacturers to employ a hybrid network, comprising a variety of different technologies[1]:

- **CAN** (Controller Area Network) bus remains the most widespread network, offering speeds of up to 1Mbps, covering everything from collision detection to dashboard controls;
- **LIN** (Local Interconnect Network) provides a low-cost solution for vehicle body applications like lights, door locks and mirror positioning;
- **MOST** (Media Oriented Systems Transport) delivers in-vehicle media via its 150Mbit/s optical fibres;
- **FlexRay** combines reliability and speed, and is used for "x-by-wire" capabilities, such as brake-by-wire.

Ethernet use remains relatively limited, and connected to functions requiring external communications—most notably diagnostics. However, this picture is set to change dramatically over the coming years.

The cost and performance benefits—along with soaring future bandwidth requirements—make Ethernet too attractive for auto manufacturers to ignore. And the OPEN (One Pair Ethernet) Alliance Special Interest Group has effectively established 100BASE-T1/1000BASE-T1 as the de-facto PHYsical layer standard for the industry, clearing the way for its widespread adoption.

Automotive Ethernet replaces the standard, 8-wire shielded twisted pair cabling with a smaller, 2-wire unshielded twisted pair.

By simplifying to a single system, reducing expensive copper and duplicated network hardware, Automotive Ethernet is some 30% lighter than equivalent mainstream technologies, improving vehicle efficiency, and reduces installation costs by 80%.

The new standard, commonly known as as 100BASE-T1 (100Mbps) and 1000BASE-T1 (1Gbps), is becoming essential as ADAS (Advanced Driver Assistance Systems) and "connected car" functions escalate demands for complexity and bandwidth.

Moreover, increasing complexity in vehicle computing, infotainment and security will mean the next-generation of connected vehicles require software updates on a regular basis. Switching to Automotive Ethernet from classic bus systems has the potential to prevent a bandwidth bottleneck[2], and transform the job from all-day garage procedure to something that can be carried out while the owner waits[3]—or even to something that can be conducted over-the-air with no need to visit a garage.

The results are impressive. BMW achieved dramatic cabling cost reductions by using Automotive Ethernet Ethernet to deliver vehicles with all-round camera coverage[4]. The company expects to make growing use of the technology as it becomes the backbone for localised CAN, LIN FlexRay and other systems by 2018.

In America, market intelligence company ABI Research agrees, predicting Ethernet penetration in new cars worldwide to grow from 1% in 2014 to 40% by 2020[5].

[1] Renesas, "Introduction to CAN" Application Note, April 2010

[2] New Electronics, "Ethernet finds use in the automotive industry", November 2013

[3] Engineer Live "Ethernet makes its way into the car"

[4] BMW Group, "Ethernet—the standard for in-car communication", September 2012

[5] Fierce Telecom, "Ethernet In-vehicle Networking to Feature in 40% of Vehicles Shipping Globally by 2020", January 2014

An Overview of Automotive Ethernet Testing

As a new technology, potentially used in safety-critical systems, Automotive Ethernet will clearly require particular scrutiny from automotive manufacturers, to safeguard customers, protect brand integrity and avoid costly and embarrassing recalls.

Crucially, 100BASE-T1/1000BASE-T1 only represents a new PHYsical interface. Everything beyond the PHY layer—such as MAC addresses—remains standard, with well-established testing methodology throughout the industry at large.

However, Automotive Ethernet has different characteristics from existing bus systems, and there remain a number of technologies that will need to be tested:

- Ethernet and Internet Protocol (Ethernet/IP)
- Applications, and their interaction with the new network
- Gateways and switches
- Protocols

(More detailed information on Automotive Ethernet protocol conformance testing is available in a separate Spirent white paper: "Automotive Ethernet Conformance Testing".

Within each area, several important characteristics will affect the system's ability to carry out different functions. For example:

- **Availability and reliability testing** across a full range of likely scenarios, to ensure consistent, predictable performance of critical powertrain, chassis and body functions
- **Quality testing** for smooth handling of media files within infotainment systems
- **Latency testing** to guarantee timely operation of ADAS equipment
- **Load testing** for high-bandwidth applications like surround view cameras

Key Test Types for the Automotive Network

Although automotive networks clearly have very specialised requirements, the broad framework for Automotive Ethernet testing can, in many ways, grow organically from well-established best practice for network testing in the IT industry.

Three types of tests are likely to prove particularly useful:

Conformance testing ensures protocols function correctly and meet approved standards. Within IT, such tests are now often taken as read, since the standards are so well established and understood that OEMs are able to rely on their vendors.

In automotive, however, Ethernet is still new and developing. What's more, manufacturers assume overall responsibility for the function of the entire vehicle, and carry the reputational damage and recall costs if things go wrong, so will understandably want to test for themselves.

Negative testing confirms how the system responds when it encounters errors, encounters unexpected or nonstandard signals, or no signal at all—while "fuzzing" rapidly tests every possible permutation close to the expected outcome.

Exhaustive negative testing is particularly important in automotive scenarios, where a vehicle must remain safe to use, whatever difficulties its network encounters.

Performance testing checks how much load the system can bear, and what happens when this limit is exceeded. For example, when faced with a sudden surge in demand for network bandwidth, can a vehicle still identify, prioritize and deliver the most important messages, such as brake function?

In some cases, standard IT industry interfaces can be suitable for automotive use. However, the requirement for hardware-in-the-loop testing, along with the ability to customise automated test runs, often means an automotive-tailored solution is required.

State-of-the-Art Test Solutions for the Automotive Market

Automotive Ethernet replaced the standard, 8-wire shielded twisted pair cabling with a smaller, 2-wire unshielded twisted pair more commonly known as 100BASE-T1 (100Mbps) and 1000BASE-T1 (1Gbps).

The **1000BASE-T1 standard** allows high speed and simultaneous bi-directional data traffic over lightweight, single-pair cable harnesses. This results in reduced weight and increased reliability due to the need for fewer cables and connectors in automotive applications.

To enable automobile manufacturers and suppliers to deliver competitive, innovative features while minimizing costs, Spirent offers the industry's first Automotive Ethernet conformance and performance test system for the new 1000BASE-T1 PHYsical Layer Standard.

With support for up to 16 individual ports for testing different kinds of PHYsical layer interfaces, copper and fiber, 10-1000Mbit/s, this test solution allows manufacturers to determine whether their data traffic is transmitted correctly and on time over the market's highest in-vehicle connectivity bandwidth.

A Vital New Challenge: Security

Above all else, the automotive industry needs to understand one key truth inherent in the rise of automotive Ethernet: Hacking is inevitable.

In coming years, as Automotive Ethernet comes into contact with more valuable and safety-critical systems, network security will become hugely significant as a safety and reputational issue for automotive brands.

Already, electronic, consumer and retail brands have experienced significant customer backlash when hackers have stolen potentially sensitive passwords or financial data. The scale of the reaction if a hacker or virus should cause, for example, widespread sudden brake failure within a particular brand of vehicle, can only be imagined.

Stuxnet: A Lesson from History

Even the most important, advanced and safety-sensitive computer systems are vulnerable to attack if not properly protected.

In 2010, centrifuges at the heart of Iran's Natanz nuclear enrichment facility started to spin wildly out of control.

Meanwhile, computer monitoring systems remained profoundly unmoved, registering the situation as completely normal. Reportedly, some 20% of Iran's nuclear centrifuges were eventually destroyed[6].

The malfunction was caused by Stuxnet; a computer virus created by US and Israeli forces that found its way into Iran's nuclear network after being hidden on a worker's USB thumb drive.

A cleverly engineered piece of malware, the Stuxnet worm self-replicated, while seeking out the systems' weaknesses and taking note of usual readings to prevent the system from recognising the problem until it was too late.

As a direct result of the cyber weapon, Iran's nuclear program has been set back several years[7]. And there is no reason why a similarly crippling attack could not befall a connected car.

[6] Business Insider, "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought", November 2013

[7] New York Times, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", January 2011

Why Ethernet Changes the Game for Automotive Network Security

Although CAN and other bus networks are theoretically vulnerable to hacking and other security risks, the specialized nature of the interface restricted the practical threat to an extremely low level.

Now, however, the standardized nature of Ethernet means that the tools and techniques to hack tomorrow's connected vehicles are freely accessible over the internet. When Automotive Ethernet becomes the backbone for the entire system, all parts of a vehicle's network can—in theory—become vulnerable to access through its diagnostic port, or even through cellular networks.

For the first time, the threat is real. To protect the safety of inhabitants, every vehicle will need multiple firewalls built in to its network. In particular, the gateway between a car's infotainment system and automotive functions will need to be validated with extreme care.

In short, the rise of Automotive Ethernet also brings the automotive industry into the front line of the IT industry's rapidly-evolving battle to anticipate and reject security threats.

Thankfully, the car manufacturers can draw upon tried-and-tested methodologies and expertise to ensure their networks are safe and secure.

To validate both specific security functionalities and overall robustness of the system, engineers should subject a network to a number of accurately simulated threats under closely controlled and observed conditions, including:

- Replicating the behavior of an **infected device**
- System attacks, using a full variety of known **hacking** approaches
- Checking for a wide variety of "**zero-day**" vulnerabilities
- Confirming the system's resistance to distributed **denial-of-service** (DDoS) attack
- Infection by **malware**, viruses, trojans and worms

Although rigorous security validation could scarcely be more important to the next generation of connected vehicles, it is easier to achieve than it might sound. The existence of trusted testing methodologies and apparatus mean automotive manufactures should be able to incorporate these within standard development tests, rather than needing dedicated specialists in house.

Next Steps

This document has attempted to set out, at a broad level, how automotive network test requirements are shifting as systems change—and in particular as Automotive Ethernet becomes more prevalent.

For managers responsible for vehicle quality, the overarching message is simple: additional procedures and new standardized tests for tier 1 suppliers are vital—and the industry as a whole urgently needs to realize the critical importance of network security.

Those tasked with establishing new test regimes may benefit from more detailed guidance. Spirent has also published a series of further white papers, covering key issues for automotive connectivity engineers when validating performance, security, applications and protocol conformance.

Our engineers have long experience of helping organisations to define and execute effective network tests, and as a member of the OPEN Alliance SIG we are working closely with vehicle manufacturers to tackle the challenges and help Automotive Ethernet deliver its full potential for the industry.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

Commitment to Innovation in Automotive

As transportation becomes more connected, and new features become more critical, systems designers, OEMs and suppliers need to verify their operation at all stages of development. Spirent is working with government agencies and laboratories, standards bodies and commercial organizations to help create innovative new systems and features.

Spirent's lab test solutions are perfectly suited for evaluating performance of the latest technologies. As new communication services and applications are launched, Spirent provides tools for service management and field test to improve troubleshooting and quality.

Unmatched Range of Test Solutions

Spirent's test solutions help verify that automotive networking and communication systems perform as intended. We offer a wide range of solutions for network, connectivity, and wireless/ RF testing ensuring new systems conform to regulations, meet customer expectations, and deliver market-leading performance—supporting the entire development process, from R&D to production and after-market.s

For more information on solutions related to testing connected car technology and applications, visit: https://www.spirent.com/Automotive

spirent™
Promise. Assured.

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defense
info@spirentfederal.com | spirentfederal.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev D | 03/20