Automotive Ethernet: The Future of Autonomous Vehicles

Future Development of Autonomous and Connected Driving

www.EmbeddedSystemsEngineering.com
A NEW AGE IN EMBEDDED PROCESSORS

EPYC™ EMBEDDED 3000 AND RYZEN™ EMBEDDED V1000

www.amd.com/embedded
IN THIS ISSUE

CONTENTS

EMBEDDED SYSTEMS ENGINEERING

Special Features

Engineering Automated Driving Systems for Safety
By Chip Thurston, Crystal Group Inc. 3

The Network is the Car
By Dr. Stan Schneider and Bob Leigh, RTI 5

Future Development of Autonomous and Connected Driving
By John Koon, Contributing Editor 8

Automotive Ethernet: The Future of Autonomous Vehicles
By Curtis Donahue, University of New Hampshire InterOperability Laboratory 11

ISO 26262 and You
By Jörg Grosse, OneSpin Solutions 14

Leaking Cars Lead to Sunken Reputations
Jeremy Correale, ON Semiconductor and Alan Hansford, RFMicron 16

Product Showcases

Design Tools

Prototyping

Total Phase, Inc.
A2B Bus Monitor - Level 1 Application for Promira Serial Platform 18

Teledyne LeCroy Teledyne LeCroy Automotive Solutions 19

Verification

Teledyne LeCroy
Teledyne LeCroy Automotive Solutions 19

Embedded Systems Engineering is published by Extension Media LLC, 1786 18th Street, San Francisco, CA 94107. Copyright © 2018 by Extension Media LLC. All rights reserved. Printed in the U.S.
Automated vehicles (AVs) of all types—including self-driving cars on city streets, trucks on military bases and the open road, and various unmanned platforms on land, at sea, and in air—are poised to transform transportation. The automotive market is on the cusp of significant change, enabled by innovative automated driving system (ADS) technologies; yet, widespread deployment hinges almost entirely on safety.

A single ADS mishap can have far-reaching implications, adversely affecting the acceptance and adoption of autonomous vehicles worldwide. Destruction of property and loss of life caused by any manner of ADS failure will not be tolerated, by the public, regulatory bodies, transportation officials, or lawmakers—all of whom seek assurances from automotive manufacturers that the vehicles, including all essential systems, can be trusted to perform reliably no matter what they might encounter on the road.

Predictable, repeatable performance over time is integral to safety, which in turn builds trust. A single unfortunate event could slow, set back, or even bring an abrupt end to the advancement, adoption, and acceptance of autonomous driving systems and threaten the entire global autonomous vehicle industry. Automated driving system failures are not an option and must be avoided, through the use of systems specifically designed to be durable, offer high availability, and perform reliably in various operational environments throughout their life cycles.

BEST PRACTICES AND GUIDANCE
Transportation safety experts are encouraging autonomous vehicle and automated driving system manufacturers to benefit from lessons learned in the military and aerospace market. Best practices include the adoption of industry standards and systems engineering practices successfully employed for decades in aerospace and defense programs, according to the latest guidance from both the U.S. Department of Transportation (DoT) and the National Highway Traffic Safety Administration (NHTSA).

DoT officials issued Automated Driving Systems 2.0: A Vision for Safety, voluntary guidance that encourages best practices and prioritizes safety to help pave the way for the safe deployment of advanced driver assistance technologies. In it, officials encourage technology companies working on ADS to adopt guidance, best practices, design principles, and standards from industries such as aviation, space, and the military.

Military and aerospace vehicles and vehicle-based electronics are renowned the world over for being built to work reliably, without fail, over a long operational life in even the most challenging applications, rough terrains, and extreme environments. For example, the military continues to rely upon the Boeing B-52 Bomber military aircraft, currently in its sixth decade of service and expected to serve through 2045, while NASA’s Voyager 1 spacecraft is still receiving commands and communicating data, more than 40 years into its mission, from the harsh, radiation-rich environment of space.

OPERATIONAL ENVIRONMENT
Transportation safety specialists also stress the importance of designing and validating ADS specifically for the entire operational design domain, defined as the specific environments in which the automated system is designed to operate, including roadway types, speed range, and environmental conditions, such as weather.

Military and aerospace organizations, including the Department of Defense (DoD) and NASA, learned decades ago that traditional computer and electronics systems would soon become ineffective, work only...
s sporadically, or completely fail to function in the field. Consumer- and enterprise-level systems are largely designed to operate in climate-controlled, protected office environments and, when deployed in the field, typically cannot withstand and will succumb to various environmental elements, such as: shock and vibration, drops, hot and cold temperature extremes, dust and dirt, water and humidity, and snow and ice.

These and other environmental factors threaten computer and electronics reliability, which is inextricably linked to safety. Mission- and safety-critical projects, therefore, require computer and electronics systems to be protected from the elements. The most effective, efficient, and economical way to ensure high reliability, particularly for ADS expected to function daily on everything from highways to city streets to the roughest back roads in all kinds of weather, arguably is: to use computer and electronics systems that are built rugged from design and development, through meticulous manufacturing and testing, to deployment in modern autonomous vehicles of all types in various locales.

AUTONOMOUS INNOVATIONS

Today’s savvy automotive and automated driving system manufacturers recognize the value that long-time, trusted military and aerospace suppliers bring to the AV market, including: field-tested and proven technologies, standards and requirements compliance, experience, and expertise. Many are, therefore, proactively seeking out and partnering with technology companies that have extensive experience delivering rugged computer and electronics systems designed to meet strict industry standards and operational requirements and built to last in a variety of demanding applications and challenging environments.

Technology leader Intel Corporation partnered with Iowa-based Crystal Group Inc.—designer/manufacturer of rugged computer hardware, member of the Intel Internet of Things (IoT) Solutions Alliance, and award-winning Intel Technology Platinum Provider—to design, develop, manufacture, and test a robust, rugged, and reliable high-performance computer crafted specifically to speed time to market of autonomous vehicles and automated driving systems. Crystal Group’s technical staff applied decades of experience engineering systems to meet strict military small size, weight, and power (SWaP) requirements to pack the processing power and data storage capacity of a high-end server in a 3U high-performance embedded computer (HPEC) while reducing power consumption and limiting system temperature rise.

That award-winning AV computer designed in close collaboration with Intel formed the basis of the new Crystal Group Rugged Autonomous Computer Equipment (RACE™) line that is helping to accelerate AV and ADS development, testing, and deployment to bring innovations to market faster. The Crystal Group RACE0161 Rugged Server provides automaker OEMs with compute power, data-handling and Internet of Things (IoT) capabilities, and data storage capacity in a compact, rugged solution capable of withstanding harsh environmental conditions, including potholes, washboard roads, temperature extremes, and collisions that are likely to cause traditional systems to fail.

Specifically designed for unmanned and autonomous driving vehicles, the Crystal Group RACE0161 provides the horsepower AV and ADS projects need with dual Intel® Xeon® Scalable Processors (Skylake) to deliver a unique, turnkey AV/ADS computer with industry-leading compute and IoT capabilities. The rugged server combines robust I/O, multiple GPU capacity, dual Intel Xeon CPUs, sophisticated thermal management, and other high-quality components stabilized in a rugged, aluminum enclosure measuring just 6.5 x 14.1 x 15.6 inches and weighing 30 to 40 pounds. Providing superior performance per watt, the high-performance server can operate off a 12-volt (12V) car battery without the need for AC/DC power conversion and does not require costly and time-consuming power modifications to convert 12V power systems to existing 24V power systems.

Crystal Group’s RACE product line, including the RACE0161 and vehicle-specific development kits, is designed to deliver speed, agility, and quality in a single, turnkey package, helping AV and ADS manufacturers take advantage of the latest technology advances while speeding the pace of development. Crystal Group’s RACE0161 is garnering global industry attention for its potential to put AV and ADS projects on the fast track by speeding time to market, ahead of competitors, with the added confidence that comes with a military-grade, rugged, reliable solution.

HIGH RELIABILITY FOR SAFETY

“From reducing crash-related deaths and injuries, to improving access to transportation, to reducing traffic congestion and vehicle emissions, automated vehicles hold significant potential to increase productivity and improve the quality of life for millions of people,” A Vision for Safety 2.0 explains. Motor vehicle-related crashes on U.S. highways claimed 37,461 lives in 2016, DoT research indicates, noting that 94 percent of serious crashes are due to dangerous choices or errors people make behind the wheel.

“Technology can save lives,” transportation safety officials affirm, with the help of highly reliable, fail-safe automated driving systems tailored to fit the application and the environment. “Thanks to a convergence of technological advances,” A Vision for Safety 2.0 reads, “the promise of safer automated driving systems is closer to becoming a reality.”

Self-driving cars bring the promise of greater energy conservation, lower emissions, added convenience, and roads that are both safer and less congested. To fully realize this vision, automotive manufacturers and autonomous vehicle makers are opting to benefit from established standards and lessons learned in mission- and safety-critical military and aerospace programs. Through collaboration with experienced, trusted industry partners with proven, field-tested, military-grade products, services, and technologies manufacturers of autonomous vehicles and automated driving systems can bring their innovations to market faster. And with the added confidence that comes with rugged, reliable systems built to last in even the most extreme environments.

Chip Thurston is Chief Architect & Technical Director Crystal Group Inc. Thurston joined Crystal Group in late 2000, holding various leadership roles in engineering. Thurston pioneered advanced rugged technology for many major computing systems that are currently being used by NASA, Intel®, U.S. Armed Forces, and major automotive manufacturers. A native of Cedar Falls, Iowa, Thurston holds an AA in MIS/CIS and a BA in Business Management.
The Network is the Car

How data centricity connects with Artificial Intelligence in Autonomous Vehicles.

By Dr. Stan Schneider and Bob Leigh, RTI

An autonomous car combines vision, radar, LIDAR, proximity sensors, GPS, mapping, navigation, planning, and control. These components must combine into a reliable, safe, secure system that can analyze complex environments in real time and react to negotiate chaotic environments. Autonomy is thus a supreme technical challenge. An autonomous car is more a robot on wheels than it is a car. Unlike current cars, autonomous vehicles (or “carbots”) must suddenly be Artificial Intelligence (AI)-capable computers.

Of course, there are millions of lines of software in today’s cars. But most is embedded in Electronic Control Units (ECUs). ECUs may perform complex functions, but their interactions are minimal. That design—and indeed the entire supply-chain model—doesn’t extend to autonomous drive. Autonomy requires richer connectivity between components and increasing the connectivity of the existing designs is impractical without an entirely new architecture.

The new generation of autonomous vehicles also requires distributed computing. Even with extremely-fast processors, distributed computing has many fundamental advantages over centralized designs. Most importantly, distributed systems are more modular. That helps optimize designs; for instance, pairing computing with sensors matches the software to the hardware and eases tuning. Plus, distributed systems can more easily support redundancy, increasing reliability. These advantages become critical at higher levels of autonomy.

To address these challenges, data-centric architectures are becoming the new standard for highly autonomous vehicles. Data centricity enables and controls complex data flow. It greatly simplifies component interaction. It reduces lines of code in the ECUs. And it directly supports AI modules.

DATA CENTRICITY

Data centricity is an architecture formed from participants that communicate only with the data infrastructure. Data-centric communication systems contrast with object-oriented systems (where objects communicate), message-oriented systems (where participants send messages to each other), and service-oriented architectures (where participants connect to services). Participants in data-centric systems are decoupled from all other participants in time, space, and flow. Data-centric connectivity is also called a “databus,” defined by the Object Management Group (OMG) Data Distribution Service (DDS) standard.

Databases are also data centric. However, a database implements data-centric storage, while a databus implements data-centric communication. The key difference: a database searches old information by relating properties of stored data. A databus finds future information by filtering properties of the incoming data.

DDS implements the virtual abstraction of a “global data space”—all data appears to be available everywhere. In reality, of course, that is not possible. But, by asking every application to specify what it has or needs, how much data that is, and how often it can produce or consume it, the databus can make it appear so. Thus, every application simply provides data it knows into the space and gets the data it wants from the space. It’s naturally parallel; all the data is logically everywhere whenever anything needs it.

Figure 1: Database vs Databus. In a data-centric architecture, applications communicate only with the data infrastructure, not with each other. A database implements data-centric storage that finds the right old data through search. A databus implements data-centric sharing that finds the right future data through filtering. Both technologies make system stem integration much easier, supporting larger scale, better reliability, and application interoperability.
The databus is elegant and powerful. Applications automatically discover any data, along with metadata like timestamps, types, and units. Any application can join, leave, add data, or remove data at any time. The databus guarantees data delivery rates and maximum allowed delays. Applications can request notification of changes in specified timeframes. History is available on request. All communications are peer-to-peer, allowing operation at full wire speeds. It does not require servers, so there are no servers to locate, configure, provision, reboot, choke, or fail. It scales well; adding new flows does not disturb current flows. And, it incorporates fine-grained security; only applications with the right permissions for specific dataflows can participate. Just as the database enables complex enterprise applications, the databus enables complex intelligent systems. Both do that, fundamentally, by simplifying applications through data management.

DATA CENTRICITY AND AI

The DDS “all data everywhere” abstraction simplifies AI integration. In fact, the databus concept started in autonomous systems at the Stanford Aerospace Robotics Lab. It has unique properties that map well to the challenge. Table 1 summarizes the challenges and approach.

Perhaps most importantly, a databus supports many dataflows with one abstraction. Most earlier designs require a separate technology for every flow. For instance, older systems would send the extreme throughput of video over a streaming protocol but use a specialized real-time bus for small but frequent control signals. Worse than the hardware, this also forced a change in abstraction. That makes it hard to write software that can fuse the sensor sets.

Highly autonomous systems make this much more challenging. Carbots combine many direct and derived sensors, perception modules, intelligence, feedback control, and off-vehicle communications. Combining all these data through traditional designs is messy.

DDS excels at dataflow control. Distributed architectures are much easier with an abstraction that delivers the right data to each module.

At lower levels of autonomy, designs can use a centralized design that sends all data to a single central computer. Consider, for instance, the perception system. A key need is to “fuse” data from many sensors into a single common understanding of the situation. The easy way to access all that data is to get it all to the same place for processing. Thus, if the vehicle has an array of cameras and proximity sensors, each would send the raw video and data streams to the central processor. This simplifies computing. Of course, the processor becomes a choke point and single-point-of-failure. Worse, it requires a lot of data transfers and dedicated video wiring for each camera.

For higher levels of autonomy, this design breaks down. Rather than send all the raw data to one central box, it’s more effective to pre-process the data closer to the sensor. This is often called “early” or “hybrid” fusion. The databus is a good fit for this design; its data-centric virtual “global data space” abstraction is a powerful substitute for actually sending all data to a central node.

THE FUTURE OF AUTONOMOUS SYSTEMS

Autonomy requires complex software integration in the vehicle. That’s difficult to do by combining ECUs. Thus, OEMs are increasingly looking to in-house software teams. DDS provides a powerful standard to enable that effort. Most carbot designs use DDS directly. However, it also underlies other architectures, such as ROS2 and soon, AUTOSAR.
Of course, DDS is far more than an in-vehicle technology for automotive systems. RTI Connext DDS, for instance, has over 1000 designs in the Industrial IoT including medical, oil & gas, naval, avionics, air-traffic control, hyperloop, metro transit, and robotics applications. Therefore, DDS is also a good fit to the off-board needs of autonomous drive systems. Its increasing traction across the broad sphere of smart machine applications makes it a good decision for the future.

Dr. Stan Schneider is CEO of Real-Time Innovations (RTI), the Industrial Internet of Things connectivity company. Schneider serves as Vice Chair of the Industrial Internet Consortium (IIC) Steering Committee. He also serves on the advisory board for IoT Solutions World Congress, and chairs OpenFog’s Fog World keynote committee. He was named Embedded Computing Design’s Top Embedded Innovator Award 2015 & IoTOne’s top-10 most influential in the IIoT 2017. He holds a PhD in EE/CS from Stanford.

Bob Leigh is director of market development, autonomous vehicles at RTI. He brings over 15 years of experience developing new markets and building technology companies to his role. Leigh graduated from Queen’s University with a degree in Mathematics and Engineering and has used his education in control and communication systems to engineer embedded solutions for a variety of industries including energy, manufacturing, and transportation.
Future Development of Autonomous and Connected Driving

SAE L5 will be a reality, but that reality will vary from city to city and from country to country.

By John Koon, Contributing Editor

INTRODUCTION
Autonomous driving is here, at least on a limited scale. In fact, you experience autonomous driving (AD) all the time. At the San Francisco Airport, when you get on the monorail to move between different terminals, you are experiencing autonomous driving. Even though it is remotely controlled, there is no human driver on board. We cannot go to a car dealer today to buy a fully autonomous car, but that is about to change. However, with the California Department of Motor Vehicles (DMV) announcement that starting April 2, 2018, automakers can test drive a fully autonomous vehicle with no human onboard, we marked an historic milestone. The manufacturer must, however, obtain a driverless testing permit from the DMV and meet the permit requirements. Today, there are already technologies to aid partial autonomous driving. So, what does full autonomous driving mean?

AUTONOMOUS DRIVING
When describing autonomous driving most people (and the DMV) use the Society of Automotive Engineers (SAE) International’s standard J3016, which defines five levels of autonomous driving (not including Level 0, which is no automation). The following briefly defines the five levels of autonomous driving:

- **Driver Assistance (Level 1)** - the vehicle provides a specific function including acceleration and steering while the driver is responsible for the remainder of driving requirements.
- **Partial Automation (Level 2)** - the vehicle provides assistance in additional functions like steering, acceleration/deceleration and auto-braking based on sensors detecting the driver’s environment.
- **Conditional Automation (Level 3)** - the vehicle can drive itself, but with a driver that monitors the situation and can take over at any time.
- **High Automation (Level 4)** - the vehicle can take over all aspects of driving on surface streets.
- **Full Automation (Level 5)** - this is the highest level of automation. The vehicle can take over the driving function completely. This is the goal that all manufacturers are aiming for.

CONNECTED DRIVING WITH VEHICLE-TO-VEHICLE (V2V) TECHNOLOGY
In tandem with the autonomous driving fever from the automakers and manufacturers, the National Highway Traffic Safety Administration (NHTSA), the government agency responsible for motor vehicle safety, is working with the Department of Transportation (DOT), the automotive industry, and academic institutions to research Vehicle-to-Vehicle (V2V) Communications. NHTSA will be proposing regulations to require vehicles to implement V2V, with the ultimate goal of eliminating traffic accidents.

V2V uses dedicated short-range radio communication (DSRC) to communicate with other vehicles to exchange information such as a vehicle’s speed, heading, and braking status. A vehicle equipped

1. [https://www.youtube.com/watch?time_continue=37&v=3z091CqmiLU](https://www.youtube.com/watch?time_continue=37&v=3z091CqmiLU)
with V2V will be able, for example, to detect that a vehicle in front has applied its brakes and is slowing even before the driver can detect what is happening ahead. DSRC are secured, wireless two-way communications that allow vehicles to interact within approximately 300 meters using the 75 MHz band of the 5.9 GHz spectrum, which has been allocated by the FCC for Intelligent Transportation Systems (ITS). NHTSA estimates that using “intersection movement assist” (IMA) and “left turn assist” (LTA) can potentially reduce accidents and related injuries by 50%.

THE RACE TO AUTONOMOUS DRIVING

In recent years, many of the top manufacturers have rushed to join the race to offer autonomous driving. They include the alliance of Intel, Mobileye (now part of Intel) and BMW. Separately top automakers like Toyota, General Motors and many others are joining the race.

Intel, the largest silicon manufacturer, has developed the advanced driver assistance systems (ADAS) using many of its processors to support camera, sensors, graphics, and audio to provide speed status, steering information, graphics and audio warnings. With the Intel/BMW alliance, the goal is to offer fully autonomous (SAE L5) vehicles in the coming years.

In 2015, Toyota Research Institute, a wholly owned subsidiary of Toyota Motor North America, began to focus on advanced technology for autonomous driving. At the recent Consumer Electronics Show (CES 2018), Toyota Research Institute (TRI) demonstrated its next-generation automated driving research vehicle on a Lexus LS 600hL. The new Platform 3.0 can detect a 360-degree perimeter using four high-resolution light detection and ranging (LIDAR) scanning heads. (More info on Luminar LIDAR below).

Another major automaker in the autonomous driving business is General Motors. Recently it filed a petition with the DOT for a SAE L4 Cruise AV, which will be able to operate safely on the road without a driver, pedals, or steering wheel by 2019. As early as 2015, GM started testing AD in the streets of San Francisco, which was much more challenging than doing AD in a rural area.

NEW INNOVATIONS PROPEL AUTONOMOUS DRIVING

Improving critical technologies has helped propel autonomous driving in ways not possible before. These technologies include deep learning/artificial intelligence (AI), sensors including light detection and ranging (LIDAR) and radar, new cameras, and new silicon solutions.

Deep Learning / artificial intelligence (AI) technology is fueling autonomous driving. NVIDIA, a leader in graphic processor units (GPUs) provides super-fast GPUs to help cars learn how to drive. The GPU technology can learn much like a human driver does and can improve its driving skill over time. Many automakers are using the technology to achieve autonomous driving including VW, Volvo, Audi, Tesla and Mercedes-Benz. A competing technology offered by Mobileye (acquired by Intel for $15.3 billion in 2017) includes additional software for autonomous driving, Mobileye (Intel) is working with multiple automakers including BMW, Audi, and Honda to produce SAE L3 autonomous cars (AC) starting in 2019 with the goal of launching an SAE L4 AC in 2020. Computer giant IBM is utilizing AI in AD with Watson, its AI engine, to propel an electric bus.

One breakthrough is the advancement of LIDAR technology comes from Luminar. Most other LIDAR or equivalent technologies cannot distinguish between objects with similarly dark or bright colors. However, the Luminar LIDAR sensor can, at 75 MPH, detect a 10% reflectivity object, like a black car or tire on the road, from a distance of 200 meters, providing seven seconds of reaction time. It operates at 1550nm wavelength, and compared with other LIDAR solutions, offers resolution that is 50 times greater with a range that is 10 times longer. Toyota has incorporated the Luminar technology in its future autonomous driving solution.

Mentor Graphics, a Siemens business, provides automotive networking solutions to many carmakers with hardware and design tools in the automotive areas of connectivity, electrification, autonomous driving and vehicle architecture. For autonomous driving, signals from various sensors including radar, LIDAR, vision, and others are fed to a central processing system. Mentor provides the DRS360 platform which captures, fuses and utilizes raw data in real time for autonomous driving and is ISO 26262 ASIL D-compliant.

NXP has been providing semiconductor and software solutions to the automotive segments for many years. (Qualcomm has offered to acquire NXP). Its solutions cover Driver Replacement and Connectivity, In-vehicle Experience, Body and Comfort, and Powertrain and Vehicle Dynamics. Its S32 platform is a scalable automotive computing architecture to support autonomous driving. The platform includes S32 MCUs and MPUs, design studio and an automotive-grade software developer’s kit (SDK). Recently it introduced the NXP BlueBox, a development platform that makes it easier for developers to achieve SAE L3 autonomous driving. The kit includes vision and sensor fusion processors, embedded compute processors, and a radar microcontroller.
SAE Level 2 (and beyond) autonomous driving requires many sensors including radar. In theory it would require multiple silicon chips and a transceiver with an external MCU or DSP to process the radar data. Texas Instruments, a provider of advanced driver assistance systems (ADAS) to the automotive segment for many years, offers the AWR1642 device, which is a single-chip Frequency Modulation Continuous Wave (FMCW) radar sensor capable of operation in the 76- to 81-GHz band with 4 GHz available bandwidth. Based on CMOS, it also includes a transceiver with an external MCU or DSP and Arm Cortex-R4F-Based Radio Control System. This single chip solution provides a compact solution for future autonomous driving.

WHAT WILL THE FUTURE LOOK LIKE?

We witnessed a historical milestone when the California Department of Motor Vehicles announced that starting April 2, 2018, automakers can test drive a fully autonomous vehicle with no human onboard. With the National Highway Traffic Safety Administration (NHTSA) drafting regulations to require the automotive industry to implement V2V, we are one step closer to real, safe autonomous driving. With break-through technologies like deep learning, LIDAR and companies like Cypress, Mentor, NXP and Texas Instruments offering advanced autonomous driving solutions, the industry is moving forward fast. With major corporations such as Intel, Toyota, GM and the like investing heavily and claiming autonomous driving production models coming in the next few years, what will the future of autonomous driving look like?

Don’t expect that tomorrow you will hear an announcement from an automaker that model AD-X is now available, so you can just relax and leave the driving to the computer. Instead, you may hear that the city of Petaluma, Calif. has announced that the city will now run a driver-less bus from 9am to 5pm, and that residents are welcome to try it. Or areas of central California will announce that effective May 1, 2020, all fields will be tilled by machines without human interaction. Full autonomous driving will come, and the progress to date is remarkable. But you will need to be patient for a little while longer.
Automotive Ethernet: The Future of Autonomous Vehicles

Understanding how the new Automotive PHYs differ from other BASE-T PHYs matters. Here's why:

By Curtis Donahue, University of New Hampshire InterOperability Laboratory

INTRODUCTION

From a broad market perspective, Automotive Ethernet is a joint effort of the Automotive and Networking industries to modernize, simplify, and expand the capabilities of vehicles by improving data communications inside vehicles. The key factors that led the Automotive industry to start this effort are the need for higher bandwidth, shifting of architectures to a centralized backbone, and guaranteed latency. Reducing the complexity of today’s vehicle network infrastructure, which commonly has up to eight different networks, is also a key driver. The complexity of handling so many different networks has a huge impact on the cost of today’s vehicles. Not only does the need for specialized skill sets for each networking type add expense, so does the difficulty of managing legacy software/firmware, with resulting incompatibility and inability to reuse parts. Because these improvements required a dedicated physical layer network, the industry widely recognized the strength of Ethernet as an ultra-compatible and flexible network that could handle the requirements of the Automotive industry. In 2014, the IEEE and the Automotive industry began efforts to make Automotive Ethernet a reality.

WHAT MAKES IT ‘AUTOMOTIVE’?

‘Ethernet’ is one of the most ubiquitous LAN communication technologies in the world, but how an Ethernet network is implemented and physically represented can vary depending on the application. The IEEE 802.3 Ethernet standard has more than 100 clauses, each defining different protocols or physical layers (PHY) designed to cater to the many industries that have embraced Ethernet for the last 40+ years. When asked to describe ‘Ethernet’, most people probably associate the plug on the back of their desktop PC and the Cat 5e network cable that connects to it. This form of Ethernet is one of several BASE-T PHYs that have been installed in office buildings for the better part of 30 years. These technologies all use the RJ-45 form factor (computer plug), designed to operate on Category cabling up to 100 meters, and can transfer data up to 10Gbps (but most installations are 1Gbps or slower). There are also the high-speed Ethernet implementations used in server farms that can transfer up to 10Gbps but have a reach of less than 10 meters over twinaxial based copper cable and implement different connectors. However, all Ethernet system models share the same media access control (MAC) definition (only the physical layer and transmission medium differ). So, all upper layer functionality is agnostic to the specific application being implemented. Another way to say this is that all Ethernet regardless of the physical medium use the same frame format. This is one of the key benefits of Ethernet.

‘Automotive Ethernet’ typically refers to one of two IEEE PHY definitions. Either IEEE 802.3bw, the 100Mbps PHY, or 802.3bp, the 1Gbps PHY, specified in Clause 96 and Clause 97 respectively. While these PHY types are commonly referred to as 100Mbps and 1Gbps Automotive Ethernet, their official IEEE PHY name is 100BASE-T1 and 1000BASE-T1. ‘BASE-T’ meaning a baseband technology that operates over a copper twisted pair medium, and ‘1’ specifying the number of differential pairs needed within the copper link segment. Both were developed within the IEEE at nearly the same time, and the use case for each is quite similar so they share several design features. These include a 15-meter reach, full duplex operation over a point-to-point single unshielded twisted pair (UTP) architecture, and three-level pulse amplitude modulation (PAM3) line coding.

But why not just reuse the existing Ethernet definitions? Each protocol and PHY defined in the IEEE 802.3 standard is developed such that its implementation can be flexible to avoid limiting the technology to a specific application space. That being said, there also needs to be a starting point with use cases proving broad market potential, a distinct identity, and technical feasibility. The Automotive industry determined that existing Ethernet technologies didn’t meet all its needs as a cost-competitive option. First, cars are not 100 meters long, so the traditional BASE-T PHYs that are built into our laptops were over-designed in terms of reach for this specific PHY. Second, the envi...
environmentally conscientious climate of the world demands fuel-efficient vehicles, and one of the simplest ways to improve fuel economy is to reduce a vehicle’s weight. Much to the IEEE community’s surprise, the third heaviest component in a car is the cable harness (heaviest is the engine, and second heaviest is the chassis). The Cat 5e cable used with BASE-T PHYs have four twisted pairs (eight wires), so one of the requests was to define the Ethernet network over a single twisted pair, leading to a weight (and therefore cost) reduction compared to Cat 5e cabling (Figure 1). Lastly, the environment inside a vehicle is drastically different than the office or home. Not only do the electronics and cabling need to withstand dirt, oil, grease, freezing temperatures, and blistering heat, but there are also electromagnetic interference (EMI) concerns so that the other circuitry in the vehicle isn’t compromised from radio frequency (RF) radiation of the Ethernet network. This is very different than the typical office and data-center environment considered by earlier Ethernet standards.

There are three functions in the IEEE BASE-T1 PHY architecture (Figure 2) that have distinct capabilities and encompass all of the mandatory conformance requirements: physical medium attachment (PMA), physical coding sublayer (PCS), and PHY Control (function within the PMA).

**CONFORMANCE TESTING FOR AUTOMOTIVE ETHERNET PHYS**

As if the differences between the Automotive market and other Ethernet markets isn’t apparent by now, there’s also literally no room for error. In the office, it’s a slight annoyance if a data packet is received in error; in a self-driving car it could mean the difference between stopping at a traffic light or running a red light into oncoming traffic. With self-driving fully autonomous vehicles all but a reality, Automotive OEMs have countless safety regulations they need to prove can be maintained while a person is not under direct control of the vehicle. So, conformance test specifications have been defined for every aspect of the vehicle’s performance, including the Ethernet components that are installed.

The test equipment needed for the transmitter distortion test setup (Figure 3) consists of a real-time oscilloscope, differential probe, and waveform generator. All of these are common in test houses and used for most time domain test cases. However, the injected sine wave needs to be synchronized with both the oscilloscope sampling clock and DUT transmit clock to guarantee that the clock domains aren’t misaligned. Not doing so will unintentionally add distortion into the system and result in inaccurate distortion values. There are two commonly used methods to properly frequency lock all the clocks within the test setup: (1) synchronize the test equipment to the DUT’s 66.67 MHz transmit clock (TX_TCLK), or (2) provide the DUT an external reference clock that is generated from the test equipment. In either scenario the tester will need access to the TX_TCLK and the ability to probe it, or the option to provide an external clock source to the silicon. So, this requires the silicon vendor to provide such hardware features to properly characterize a PHYs transmitter distortion. This isn’t always the case. The IEEE standard does not define a test method for this scenario. To resolve this, recently some T&M vendors have implemented clock and data recovery (CDR) functionality into their oscilloscopes, which removes the need to have direct access to the DUT’s TX_TCLK.
PHYSICAL CODING SUBLAYER AND PHY CONTROL CONFORMANCE TESTING

The PCS and PHY Control test specifications are less straightforward. These sublayers are the digital logic within the PHY and are typically governed by transmitter and receiver state machines that define specific state behavior and timing requirements for each operation. Rather than calling for oscilloscope measurement of standardized test patterns transmitted by the PHY, these test cases require that the DUT successfully achieve a link with a test station that behaves as if it is a PHY. Meeting this requirement means that the test station must be able to encode a specific test sequence into the PAM3 signalling. What’s more, the test station must also decode the PAM3 signal the DUT transmits. To achieve these goals, the University of New Hampshire InterOperability Laboratory (UNH-IOL) created an FPGA-based test tool (Figure 4) that performs the necessary conversion to PAM3 signalling as well as bit-level error injection to fully stress the DUT’s receiver logic.

Ethernet PHY receiver definitions specify many requirements, but how the functionality is implemented is left to the designer. So, test sequences necessary to test conformance can vary among silicon companies. One of the least consistent PHY parameters is the time necessary to achieve a link. Typically, the number of received idle symbols needed for the DUT to reliably recover the clock of the remote PHY governs the time needed to achieve a link—making test tool flexibility to accommodate any DUT crucial. Additionally, many test cases within these conformance test specifications perform negative test conditions, meaning intentionally injecting errors within the data stream to observe how the PHY behaves. Because of this, some test cases require bit errors, erroneous PAM3 symbols, or Ethernet packets with incorrect CRC values. The test setup used by UNH-IOL (Figure 5) uses a PC with custom software to dynamically control the test sequences used to accommodate any silicon design.

CONCLUSION

While the IEEE 802.3bw and IEEE 802.3bp PHY definitions may seem similar to other BASE-T PHYS, many environmental considerations and specific use-case data was used to create these unique Ethernet technologies within the IEEE standard. Test specifications were created specifically for these new Automotive PHYS, which require specialized test tools and attention to test setup details not considered in previous Ethernet conformance testing.

Curtis Donahue is the Senior Manager of Ethernet Technologies and manages the Automotive Ethernet Test Group at the University of New Hampshire InterOperability Laboratory (UNH-IOL). His main focus has been the development of test setups for physical layer conformance testing, and their respective test procedures, for High Speed Ethernet and Automotive Ethernet applications.

Donahue holds a Bachelor of Science in Electrical Engineering from the University of New Hampshire (UNH), Durham and is currently pursuing his Masters in Electrical Engineering at UNH.
ISO 26262 and You

Why Automotive electronics suppliers will make increasing use of formal tools to meet the standard’s strict requirements for verification and satisfy supply chain demand.

By Jörg Grosse, OneSpin Solutions

A lthough standards are in play for many of the electronic products that consumers buy and use, it is rare for anyone except experts to know the details. There are partial exceptions such as USB, where users at least pay attention to which version of the standard is supported in their host and peripheral devices to ensure compatibility. This has not been the case for automobiles, although important standards exist. Until quite recently, ISO 26262 was a relatively obscure specification for the development of safety-related electrical and electronic systems within road vehicles.

Self-driving vehicles are changing many aspects of the status quo, raising a host of questions about liability, massive changes in infrastructure, and creation or loss of entire categories of jobs. ISO 26262 is right in the middle of these changes. Automotive manufacturers and their electronics components suppliers must follow this standard and will make a big deal about compliance. Even consumers might become more aware of safety requirements and demand that their new vehicles conform.

VERIFICATION CHOICE

ISO 26262 imposes stringent requirements that encompass the entire life cycle of a system, from concept phase to development, production, and decommissioning. It addresses the overall safety management process. The standard specifies two types of faults in electronic components, both of which must be fully verified. Systematic faults are introduced during development, either through human error or tool malfunction. Random faults occur during the actual operation of the device due to external effects.

Systematic faults are handled through rigorous verification and the careful tracking of specific device requirements. Formal methods are more important than ever, since only they can provide mathematical certainty of correctness. A key characteristic of formal tools is the ability to examine design behavior exhaustively, without the need for input stimuli, and to prove that the design never deviates from its intended function. Formal tools don’t just find hardware design bugs; they can provide proof that no further bugs exist.

Simulation tools cannot achieve this level of precision, although there are some types of behavior that are best verified with simulation or emulation. The choice of which behaviors to verify with simulation and which with formal methods is one of the elements of a verification plan, the heart of any electronic development project. Chips for automotive electronics can be highly complex, making verification a long and difficult process. Per ISO 26262, this process must be both rigorous and effective at eliminating systematic bugs.

VERIFICATION FLOW

Figure 1 shows a typical verification flow for large, complex designs. The project begins with the requirements for the end product, typically written by the architecture and product management teams. As...
the design commences, each requirement is implemented by a series of features. In turn, the verification of each feature is broken down into a series of goals that must be met during the verification process. The list of goals is the basis for the project verification plan.

As part of the plan, the verification team decides which methods and tools are best suited to verify each feature and satisfy associated goals. For simulation, a testbench is developed, usually compliant with the Universal Verification Methodology (UVM) standard. Most of the verification is performed using pseudo-random tests that require functional coverage metrics to gauge their effectiveness. In an application such as automotive electronics with strong safety requirements, the verification team must achieve a very high degree of coverage.

Sometimes engineers will hand-write some directed tests in order to hit coverage points not easy to exercise with pseudo-random stimulus. They also are likely to measure code coverage on the design while running all automated and directed tests. Code coverage does not tie directly to intended functionality, but uncovered portions of the design may indicate redundant or spurious hardware logic, logic that cannot be exercised due to a design bug, or gaps in the verification plan.

For the portions of the chip verified by formal means, the team develops a set of assertions describing how the logic should behave. A formal model checker analyzes the design against the assertions and either reports bugs or proves agreement. For some types of analysis, formal applications (“apps”) require no assertions from the user at all. Formal tools also produce coverage metrics, some similar to those from simulation and some unique. As shown in Figure 1, the verification flow must support a range of coverage metrics to judge verification thoroughness.

It must be possible to roll up all the coverage information into a single view of verification completeness. Only a thorough verification plan, a rigorous verification process, and comprehensive coverage metrics can give the verification team the confidence that systematic faults have been eliminated and meet the high bar set by the ISO 26262 standard. Most of the verification is performed using pseudo-random tests that require functional coverage metrics to gauge their effectiveness. In an application such as automotive electronics with strong safety requirements, the verification team must achieve a very high degree of coverage.

Determining how well a chip design will handle random faults is not a trivial problem. Once again, formal methods provide a solution. Another key characteristic of formal tools, particularly relevant to safety-critical applications, is the ability to finely control the injection of faults into hardware models and analyze their sequential effects. Crucially, formal tools can perform this task efficiently, in terms of both user effort and computational demands, and non-invasively (no need for manual instrumentation of the design description). Figure 2 shows how this process works.

Formal tools can inject random faults, analyze whether faults can propagate to cause trouble, analyze whether the effects of faults can be observed, and provide metrics for hardware safety coverage. If a fault simulator is available, the work can be split with the formal tools, and results can be combined. Only with thorough application of these techniques can the verification team know that it has satisfied all aspects of critical safety standards.

Most consumers may not know or care about automotive safety requirements today, but this is likely to change as they look at moving to self-driving vehicles. Consumers may not know the details, but they will expect manufacturers to adhere to best practices. Compliance to ISO 26262 will be a badge of honor for manufacturers. Automotive electronics suppliers will make increasing use of formal tools to meet the standard’s strict requirements for verification and satisfy supply chain demand.

Jörg Grosse is product manager for functional safety at OneSpin Solutions GmbH. He has more than 20 years of experience in electronic design automation (EDA), functional verification, and ASIC design, having served at companies in Europe, the United States, and New Zealand. Grosse holds a Diplom-Ingenieur (FH) in electrical engineering from Anhalt University of Applied Sciences in Germany.
Leaking Cars Lead to Sunken Reputations

How wireless sensing can drive moisture out of vehicle assemblies

By Jeremy Correale, ON Semiconductor and Alan Hansford, RFMicron

Moisture ingress related quality issues can be a hard-to-detect, slow-burn problem for automakers—one that does not usually present a clear, immediate failure. This problem can loom large on the assembly line, where it is routine for vehicles to go through an end-of-line spray test to detect any water leaks that could represent a potential problem over the life of the vehicle.

Visual inspection methods can reveal significant leaks, but smaller leaks, often in inaccessible areas, are at best difficult, and at worst, almost impossible to find. Modern vehicle assembly methods and increasing electronic content in today’s vehicles accentuate the potential for moisture ingress and its impact on reliability.

ON Semiconductor and RFMicron have sought to address this increasingly important issue by jointly developing a unique, hands-free production turnkey leak detection system. The system employs tiny, low-cost, battery-free wireless moisture sensors placed strategically around the vehicle early in the assembly process. These sensors, read after the spray test, can support an effective way to not only detect moisture ingress problems, but also drive process improvements to eradicate the issue completely.

This article looks at the growing leak problem, its implications, and how this innovative approach looks set to solve the problem, minimize field failures, and protect automakers’ reputations.

WATER LEAKS ARE COSTLY

Water leaks are a costly problem for automakers in more ways than one. Modern vehicles have become more complex and incorporate new materials including aluminum, composites, and glues. Today’s cars and trucks feature hundreds of electronic sub-assemblies, which make them more susceptible to water damage than ever before.

Large leaks are usually quite easy to find and address, although the thicker sound-deadening foam being incorporated in vehicles can easily mask significant problems. Smaller leaks are much harder to detect and over time can lead to mold growth that has a potential negative impact on the on-board electronics as well as on the health of vehicle occupants.

Water ingress will always lead to expensive warranty claims for automakers; consumer surveys indicate that around 150,000 vehicles are recalled each year for water leak issues. With an average repair cost per vehicle as high as $5000, this equates to a hidden leak cost of $100 for every vehicle sold—not counting the value of a damaged brand reputation and the potential loss of future sales.

SPRAY AND SEEK

While vehicle design has moved on significantly and leaks are far less prevalent than in the past, it is estimated that up to two percent of vehicles leave the factory with hidden water leaks. In order to identify these vehicles before they reach the consumer, many automakers implement a two-to-five-minute soak test at the end of the assembly line.

These soak tests generally involve the vehicle being sprayed with high-pressure water jets from multiple angles to probe all of the vehicle openings and accelerate any water ingress. The magnitude of water intrusion during a test can range from large puddles accumulating in low lying areas of the vehicle, to just a few drops in the more obscure
places. The former are relatively easy to spot through traditional visual inspection methods. But the latter—especially if in out-of-sight areas such as between the inner and outer skins of the vehicle or soaked into sound-deadening material—are not.

Currently, there are several manual methods employed to detect water ingress after the spray process has finished. Some automakers use differential probes to electrically identify leaks or water contact indicator tapes that change color when damp. These methods may increase the chance of detecting a leak. However, they still struggle with penetrating the thicker foams and small interior spaces present in today’s vehicles. The most common method remains physical inspection by assembly line workers.

This manual method of inspection is prone to error, not least because the worker is also carrying out a plethora of other (unrelated) checks and inspections at the same time. Even when performed well, this method can only verify water that can be seen or felt by the worker’s hands. Any water that is hidden from view in inaccessible areas, such as behind interior trim or underneath carpet, is inevitably missed, setting up a future warranty claim.

Not only is the current method of ‘spray and seek’ unreliable, it also takes time and therefore imposes significant additional costs on the automaker.

**NON-INVASIVE LEAK DETECTION THAT IS COST EFFECTIVE AND ACCURATE**

Given the costs associated with unreliable test and inspection as well as the high costs of repairing every leak that reaches a consumer, it is no surprise that semiconductor manufacturers and automakers have been looking at alternative solutions. One innovative and dependable approach that has been developed to address water ingress in vehicles is the RFM5126 Moisture Intrusion Detection System. This turnkey solution allows automakers to determine if water has penetrated a vehicle. In addition, it shows the exact time and location of any leak. Furthermore, through storing and analyzing data from the system, statistics and trends can be developed for vehicle models and factories, allowing for effective design through process improvement.

At the heart of the integrated system, multiple tiny, battery-free, wireless water leak sensors are placed underneath the carpet, behind trim panels, and in other small hidden areas within the vehicle.

These sensors, sold under the Smart Passive Sensing™ and SPS™ brands, have an adhesive backing that allows them to be installed on the vehicle chassis, in locations prone to water leaks, at the bare metal stage of assembly. The sensors come with an option to include a water wicking tail during install that adheres to both the top of the sensor and bare metal chassis, thereby extending the range of leak detection in a specific vehicle location.

After completing all assembly, vehicles move through the high-pressure spray test, where the system flags any leaks including the small, hard-to-find ones. Drive-through portals receive data from the sensors, and sophisticated sensor monitoring software within the portals can accurately report leak locations to pinpoint and speed up any necessary rework.

**SUMMARY**

Water ingress is a significant problem for automakers costing them time on the assembly line as well as significant warranty claims and, ultimately, loss of brand reputation. Current testing methods are unreliable, as many leaks are hidden and assembly line workers making checks are often performing other tasks at the same time.

New Smart Passive Sensors form the heart of sophisticated leak detection systems that eliminate manual inspection and improve inspection accuracy.

The data collected provides the information needed to drive process improvement efforts that help the automaker identify systemic issues with the ultimate aim of eliminating the problem completely and permanently.

Jeremy Correale is Automotive Marketing Manager, ON Semiconductor. He leads the automotive segment of ON Semiconductor’s Protection and Signal Division based in Phoenix, Arizona. He is responsible for the definition and execution of the business unit’s automotive strategy revolving around a portfolio of ESD Protection and Small Signal Discretes, electronic fuses (eFuse), and Smart Passive Sensors (SPS). Correale joined ON Semiconductor in 2010 after completion of his BSE in Electrical Engineering from Arizona State University. In his free time, Correale is an active member of the Arizona-Nevada section of Society of Automotive Engineers (SAE) and enjoys racing in the occasional track day under the National Auto Sport Association.
Total Phase, Inc.

A²B Bus Monitor - Level 1 Application for Promira Serial Platform

Compatible Operating Systems: Windows, Linux, Mac OS X

Total Phase’s A²B Bus Monitor - Level 1 Application provides unprecedented access to the A²B system. By attaching the A²B Adapter Board in-line between nodes, the A²B monitor can non-intrusively sniff A²B data in real time. A²B superframes are decoded into I²C control data for easy debugging with Interrupts and GPIO handshakes correlated into the data capture, while I²S/TDM audio data is available in visual and audio formats. Besides the traditional Bus Data view, the application also offers a Node Topology view and an Audio Channels view. The Node Topology view allows quick visualization of all nodes for validating node initialization. The Audio Channels can diagnose audio channel problems. Real-time audio levels for all upstream and downstream channels can be mixed and monitored to quickly identify I²S/TDM data slot mismatch problems.

FEATURES
◆ Real-time capture and decoding of A²B bus data
◆ Node discovery and initialization tracking
◆ Node topology and configuration view

APPLICATION AREAS
Automotive, Audio

CONTACT INFORMATION
Total Phase, Inc.
2350 Mission College Blvd, Ste 1100
Santa Clara, CA 95054
USA
Tel: 1(408)850-6501
sales@totalphase.com
get.totalphase.com/a2b-bus-monitor
Teledyne LeCroy

Teledyne LeCroy Automotive Solutions

Control Busses
Automotive control busses enable communication between ECUs, sensors, actuators, etc. using well defined protocols. These protocols are deployed using electrical, optical, or wireless signaling. As the amount of data being transferred in-vehicle is rapidly increasing, control busses are evolving to meet the new demands.

Today’s vehicles utilize an array of different protocols for in-vehicle communication.

**CAN** – in-vehicle networks controlling window/seat operation, engine management, brake control, etc.

**CAN FD** – extends the bit rate of CAN via a flexible data rate

**LIN** – communication between components in vehicles, provides a cheaper alternative to CAN

**FlexRay** – utilizes two independent data channels for mission critical data transmission

**SENT** – point-to-point scheme for communication with sensors

**MOST** – electrically or optically based ring topology to transport data for infotainment

**Automotive Ethernet** – provides Ethernet connectivity in vehicles; used for infotainment, ADAS and can serve as Ethernet backbone

Common Control Bus Issues:
Serial bus protocol errors (ie: error frames or CRC errors)
Reflections caused from improper termination
Slow rise times causing timing errors in cause-effect relationships
Physical layer abnormalities – runts, glitches, etc.

FEATURES & BENEFITS
◆ Digital data extraction and graphing of CAN wheel speed information
◆ Detect a rogue message on a bus that is outside a list of specified message IDs
◆ Isolate signal integrity issues coming from a specific node on the bus
◆ Automated compliance testing of PHYs for Automotive Ethernet, USB, MOST, etc.
◆ Margin testing of different cable lengths and network topologies using eye diagrams and mask testing

TECHNICAL SPECS
◆ Oscilloscopes
◆ Mixed Signal Testing
◆ Serial Data Decode
◆ Signal Generators
◆ Protocol Analyzers

APPLICATION AREAS
Automotive Solutions

CONTACT INFORMATION
Teledyne LeCroy
27007 Hills Tech Court
Farmington Hills, MI 48331
USA
Tel: (248) 934-5999
Toll Free: (800) 553-2769
Fax: (845) 578-5985
contact.corp@teledynelecroy.com
http://teledynelecroy.com/automotive
A NEW AGE IN EMBEDDED PROCESSORS

EPYC™ EMBEDDED 3000 AND RYZEN™ EMBEDDED V1000

www.amd.com/embedded