Automotive Ethernet: Validating Conformance, Application Performance, Security, and Wireless Technology

Leveraging Ethernet in the Connected Car

Integrated computer systems are leading the way in helping automakers both meet strict conformance and auto safety standards and create marketable differentiation. Over time, automotive technology has changed from a simple internal combustion engine with wheels to an evolving combination of integrated computer systems—advanced driver assistance systems (ADAS), adaptive cruise control, hybrid engines, Internet access, and Bluetooth connection.

Automakers are looking to standard Ethernet technologies to provide a single, flexible, scalable, more cost-effective in-vehicle networking backbone. To ensure optimal design, functionality, performance, safety, security, and interoperability of these connected cars, automakers and their suppliers need comprehensive test solutions to validate devices, systems, applications, and even the entire in-vehicle network.

Automotive Ethernet Requires Ecosystem Testing

The role of testing is to verify proper functionality at each stage of system evolution. Effective testing means conducting development, integration, verification, conformance, and performance checks as efficiently, quickly, and accurately as possible. Automotive manufacturers have relied on complex and custom solutions to perform testing as they develop and integrate new technologies. The use of an Ethernet backbone now requires open, standard solutions that deliver testing across the whole automotive ecosystem. Ixia’s unique automotive Ethernet test solutions include conformance, wireless, application, and security validation.

Automotive Conformance Testing

To implement connected vehicle technology linking vehicles and mobile devices to each other and to the transportation infrastructure, the equipment and applications must meet minimum conformance requirements, perform to common technical standards, and interoperate with one another. Testing the automotive Ethernet network or module/component with a solution that reproduces anything less than a realistic environment introduces risk, slower product development and deployment, and lower network service quality. Ixia’s conformance test solution minimizes the risk by enabling quick validation of the network, services, and individual elements.

Automotive Wireless Testing

With drivers and passengers increasingly using personal devices in their vehicles, automakers must ensure their new designs can function as another node on the network. Testing must verify connectivity within the vehicle to both onboard systems and sensors and user devices—and beyond the vehicle, to mobile data services. These include checking Wi-Fi, 3G, and LTE to ensure security in application-aware networks. Ixia has extensive solutions for testing wireless infrastructures and devices, including solutions for Wi-Fi assessment, mobile device testing, mobile backhaul testing, and LTE.
Automotive Applications Testing

The connected car user will expect multimedia applications to perform optimally over any device and network. Revenues, customer loyalty, and brand reputation all depend on it. To meet tomorrow’s stringent automotive performance requirements, automakers and service providers need a means of measuring how applications and services will perform under real-world conditions, attacks, and impairments for the connected car. Ixia offers a suite of scalable solutions for assessing and optimizing quality of service (QoS) and user experience (QoE). Our systems and services test converged multiplay services, application delivery platforms, and security systems and procedures under realistic load conditions.

Automotive Security Testing

As the complexity of automotive electronics grows to meet user demands for more services, so does the need to ensure a vehicle’s systems are fully functional and secure. But adopting more information and communications technologies in vehicles also creates new test challenges around network and information security. Additional testing is required for wireless connectivity, security and cyber-attack mitigation, and other safety-critical systems. Any system designed to protect the in-vehicle network from attack should be tested to validate the ability to detect and prevent all of the thousands of known attacks and vulnerabilities. Ixia security solutions validate systems with fuzz testing, DDoS replication, vulnerability assessment, and security capability verification.

Why Ixia?

A complete test solution—Ixia has earned the industry’s respect as the most trusted benchmarking platform for measuring performance, scale, and security and offers the highest-density 10GE, 40GE, 100GE, and 400GE testing solutions available in the industry. Ixia applies its years of expertise and Ethernet/IP award-winning solutions for conformance, performance, and security testing to solve automaker’s new Ethernet testing challenges. Ixia solutions are designed for use by vehicle manufacturers, suppliers, semiconductor vendors, and service providers to ensure conformance, performance, and security for next-generation vehicles and networks.

<table>
<thead>
<tr>
<th>Ixia Solution</th>
<th>Key Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>IxANVL—Conformance Test</td>
<td>• Validate protocol conformance to specific standards</td>
</tr>
<tr>
<td></td>
<td>• Increase interoperability between devices</td>
</tr>
<tr>
<td></td>
<td>• Identify software issues in early product lifecycle</td>
</tr>
<tr>
<td>IxLoad—Wireless Test</td>
<td>• Application QoE from the user perspective</td>
</tr>
<tr>
<td></td>
<td>• Scalability under realistic loads</td>
</tr>
<tr>
<td></td>
<td>• Assess client performance with a wide mix of devices</td>
</tr>
<tr>
<td>IxLoad and BreakingPoint—Application Test</td>
<td>• Generate both good and malicious user traffic</td>
</tr>
<tr>
<td></td>
<td>• Create high-load and stress conditions that include impairments</td>
</tr>
<tr>
<td></td>
<td>• Measure the end-user QoE in relevant metrics</td>
</tr>
<tr>
<td>IxLoad and BreakingPoint—Security Test</td>
<td>• Simulate real-world application traffic, known vulnerabilities, and attacks to validate security mechanisms</td>
</tr>
<tr>
<td></td>
<td>• Leverage library of 240+ stateful application protocols, 6,000+ real-world attacks, and 35,000+ live malware samples</td>
</tr>
</tbody>
</table>

Ixia Worldwide Headquarters
26601 Agoura Rd
Calabasas, CA 91302
(Toll Free North America)
1.877.367.4942
(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Ixia European Headquarters
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom
Sales +44 1628 408750
(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters
21 Serangoon North Avenue 5
#04-01
Singapore 554864
Sales +65.6332.0125
Fax +65.6332.0127