Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Open-Source Software In Connected Vehicles: Pros And Cons

By **Marjorie Loeb, Richard Assmus, Linda Rhodes and Paul Chandler**
(September 25, 2018, 2:21 PM EDT)

Marjorie Loeb

Richard Assmus

Linda Rhodes

Paul Chandler

Automobiles are becoming part of the internet of things. "Connected" technologies now power onboard telematics and infotainment systems, and increasingly are deployed for driver assistance and to enhance the safe operation of autonomous vehicles.

These "intelligent" vehicles rely on an ecosystem of proprietary and third-party components to gather, analyze and then react to data from both inside and outside the vehicle. In some cases, automakers and their suppliers are eschewing the development of proprietary solutions and turning to pre-existing building blocks such as open-source software, or OSS, to reduce costs, accelerate development and enhance the interoperability of connected technologies and applications.

For instance, as early as 2013, automotive companies began weighing the pros and cons of various operating systems to use as the technology platform for infotainment systems, and then adapting existing platforms or developing their own, proprietary platforms. More recently, several automakers have announced their participation in the Automotive Grade Linux community, and their intent to collaborate and use the AGL platform for infotainment systems across multiple vehicle models.[1] Some common objectives cited by such participants were:

- The need for a very capable and flexible operating system that would be able to interface with varied peripherals and not be solely dependent on a proprietary operating system managed by a third party.

- The need for a cost-effective approach to software development, the cost of which has been increasing due to the inclusion of new applications in vehicles, and thereby representing an increasing percentage of the total vehicle cost. OSS allows each automaker to reduce such costs by leveraging common building blocks over a larger vehicle population, particularly in undifferentiated or brand-neutral applications and components.

- The ability to foster more rapid innovation through collaboration.

In sum, these automakers see OSS as key to developing a base operating system that

is flexible — one that allows for continuous evolution to add features, take advantage of advances in technology and meet emerging security threats. They also believe that OSS facilitates the development of systems that are not dependent on any individual supplier or technology and, accordingly, are more resilient to changes impacting individual parts of a complex supply chain.

Furthermore, they view OSS as helping to maintain the interoperability of the hardware and software components inside the vehicle, and — with an ever-expanding ecosystem of smartphones, service diagnostic tools, external databases and analytic tools — to enhance vehicle functionality and meet consumer demand for integration with home and mobile devices.

We have written previous articles discussing the regulatory compliance and supply chain management issues raised when integrating software into a vehicle's operating systems, including the need for relationships with suppliers that anticipate continued enhancement and repairs throughout the life of the vehicle. The introduction of OSS raises a number of additional factors that should be considered, and which we discuss below.

Despite OSS being available without charge over the internet, it is not "free," and the use of OSS as building blocks must be carefully managed. For starters, OSS is provided via specific license terms — by some estimates, there are thousands of different forms of OSS licenses with varying requirements, some more burdensome than others. Of particular concern are "copyleft" or "reciprocal" licenses, that require users to make source code available to third parties.

Depending on the license in question, the scope of this sharing requirement varies widely, including in regard to how sharing must occur and what source code must be shared (e.g., only changes made to the OSS files or any code that is based on or linked to the OSS). Thus, while OSS may be an attractive tool for all of the reasons noted above, some OSS licenses may require automakers to share source code for their proprietary software that is integrated with the OSS. In addition, some OSS licenses may also require terms that may have the effect of licensing the automaker's patented technology to third parties using the OSS, or triggering termination of the OSS license if the automaker asserts its patents against third parties.

The varying OSS licenses may conflict with each other, which can frustrate an automaker's license compliance. To comprehensively assess the risk that any combination of OSS blocks may infringe or violate the license terms, one must first identify and trace the use of OSS throughout, which may involve analyzing thousands of files or lines of code contributed from numerous sources. To maintain compliance, significant due diligence is required both at the outset and each time code is changed or altered.

To complicate matters further, the use of automated software development tools, which pull pieces of OSS from the internet, may make it difficult to identify applicable license requirements before those pieces become an integral part of the code base. While scanning software and solutions may help identify embedded OSS, significant analysis is still required to evaluate the provenance of the OSS and whether its intended use raises license compliance or related concerns.

Second, for various reasons, the total cost of using OSS ultimately may not be less than the cost of using a proprietary solution. The individual building blocks are provided on an as-is basis — with no warranties for infringement, fitness for a particular purpose or other aspects. As discussed above, the complexity and costs associated with doing a comprehensive license and infringement analysis may mean users are not able to easily assess the scope of the potential risk.

Furthermore, if OSS use is extensive or deeply embedded throughout the software, or if significant resources have been spent building interfaces to integrate components (as described below), there may be no practical way to recompile the software without significant loss of functionality. If license compliance cannot be achieved, it may be almost impossible for the automotive manufacturer to perform any necessary warranty and recall repairs to software (for example, to address newly discovered vulnerabilities) after the vehicle is sold.

With respect to functionality, while the user is not paying license fees to use the OSS, significant amounts may need to be spent on designing and building necessary interfaces, and testing both the individual building blocks and the integrated system. These are costs that may have been included in the cost of acquiring a proprietary or off-the-shelf solution that has been warranted by the developer. Automakers must rigorously test components for durability and compliance with all automotive safety and quality standards. Since automakers warrant the performance of the final integrated system, they must be sure that the sum of the parts works as a cohesive whole, and continues to do so throughout the life of the vehicle.

The cost of the testing plan (as well as the feasibility of testing third party software) and the potential requirement to make improvements to the software or the newly developed or customized interfaces available to others, including potential competitors, all must be factored into the evaluation of whether, and to what extent, using OSS is in the automaker's best interest. Other costs may include the ongoing support and maintenance of OSS, whether done internally or purchased separately.

Finally, as OSS is used to power more critical systems, it is increasingly essential to protect such systems from intrusion. Ironically, some of the touted benefits of OSS — the openness and transparency that allow for easy interoperability — run contrary to traditional methods of secrecy, isolation and segmentation as means to maintaining system security. Particularly when using OSS, automakers must focus their efforts on preventing and identifying unauthorized use or manipulation, and mitigating the impact of such occurrences.

While increased transparency and openness may encourage industry participants to openly collaborate on standards to address cybersecurity and other safety issues, such collaboration will be done in front of the world — which includes hackers and others who do not share these objectives. This may require more investment in authentication and/or certification techniques, as well as ongoing monitoring services, all of which must be factored into the real cost of using and maintaining OSS.

In addition, the openness and widespread use of a common technology platform for vehicle systems means that the exploitation of a single security vulnerability will more likely reverberate through the entire ecosystem and have an increasing impact, making the vulnerability both more attractive to exploit and harder to isolate and shut down.

While OSS has been touted as a means to develop common standards and protocols, foster the ability for multi-sourced devices to communicate with each other and avoid any one device from being tied to a proprietary system or supplier, the effective use of OSS requires a careful evaluation of the total costs of deploying, maintaining and safeguarding resulting systems. A complete weighing of the costs and benefits entails identification and review of the applicable license terms of each OSS building block (including the risk of exposing proprietary software used along with or integrated into the OSS); the ability to verify the provenance, stability and performance of each block; and an assessment of the costs to support and maintain not only the individual pieces but the integrated whole.

By taking a disciplined and thoughtful approach to the use of OSS, including carefully researching the governing licensing terms, manufacturers can appropriately assess whether each OSS building block meets the functionality, stability and security requirements of its intended use.

Marjorie H. Loeb, Richard M. Assmus and Linda L. Rhodes are partners and Paul A. Chandler is counsel at Mayer Brown LLP.

[1] See Automotive News, May 31, 2017, “Toyota uses open-source software in new approach to in-car tech”; and Automotive News China, Dec. 22, 2017, "Chery, NQ Mobile to develop connected-car technology using a Linux-based operating system"; and Automotive Grade Linux press release, issued June 5, 2018, announcing additional members joining a collaborative cross-industry effort to develop an open platform for the connected car, including a number of technology and Tier 1 suppliers to automotive OEMs.