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

Adapting Supply Relationships To Embrace Disruptive Tech

Law360, New York (February 14, 2017, 10:54 AM EST) -- Building connected and autonomous vehicles requires the automotive industry, both manufacturers and traditional component suppliers, to embrace disruptive technology and work hand-in-hand with information technology providers. Bringing together these two spheres, however, will not be without its challenges. While both are well-versed in complex operating systems, they approach system development and integration from two very different paradigms and will need to bridge those differences to work cooperatively.

Marjorie H. Loeb

Linda L. Rhodes

Traditional vehicle and component manufacturers have generally worked in closed ecosystems with long, but finite, development cycles. They are accustomed to compliance with complex regulatory regimes and other safety requirements to sell primarily physical products, albeit with increasingly sophisticated software algorithms embedded in them.

In contrast, information technology providers are accustomed to operating in open ecosystems with iterative development cycles that facilitate increased speed to market. They continuously develop their products after the point of sale, with the expectation of ongoing bug fixes and updates, and ongoing upgrades to meet constantly evolving customer expectations.

Vehicle manufacturers and information technology providers have successfully collaborated to develop hardware and software applications for add-on technology such as vehicle telematics and infotainment systems. However, working together to develop technology to be integrated into the heart of the vehicle operating system, where safety risks and the consequences of a design or other defect ratchet up, and with evolving regulatory standards and specifications, will require these parties to carefully consider the allocation of roles and responsibilities for developing robust designs and performance specifications around safety and cybersecurity.

Information technology providers will need to carefully assess their ability to adapt their design, development and testing processes to comprehend a new set of compliance responsibilities. The National Highway Traffic Safety Administration's recently issued enforcement bulletin emphasizes that motor vehicle equipment includes software and software updates, including "software that enables devices not located in or on the motor vehicle to connect to the motor vehicle or its systems,"[1] thereby subjecting this whole new sphere of suppliers to its rules and regulations, including the responsibility to determine whether or not a bug or defect in their software algorithm constitutes a "safety defect" under the Motor Vehicle Safety Act.[2]

The enforcement bulletin also states NHTSA's view that the failure to provide updates that will keep systems functioning throughout the life of a vehicle could constitute a safety-related defect compelling a recall. Accordingly, vehicle manufacturers will need to adapt their product development process. The ability to provide updates to software in a secure manner to vehicles already in the field will become increasingly important to facilitate efficient warranty and recall campaigns as well as to keep pace with ongoing technology advancements and protect against increasing cyberthreats. Vehicle manufacturers will also want to allow for the integration of new suppliers to develop software applications that need to "plug and play" into the hardware or software that was part of the initial design. Commercial agreements should address the extent to which a supplier will be required to cooperate and in some cases share confidential and proprietary information with vehicle manufacturers and their other suppliers, or provide code to facilitate updates or integration of new applications.

To date, when providing add-on technologies such as telematics and infotainment systems, information technology providers have not been called to take on significant responsibility for compliance with safety regulations and have not had to assess whether an unexpected performance anomaly in their technologies poses an "unreasonable risk to safety." Nor have providers of these add-on technologies had to shoulder much risk when agreeing to provisions that hold them responsible for meeting information technology security standards, given that the vehicles' systems with which these technologies interact do not typically result in significant product liability claims. However, an agreement to assume responsibility for, and indemnify the vehicle manufacturer against, claims and related losses arising from design and performance defects is a larger risk where those defects may result in significant product liability claims or personal injury cases.

To successfully collaborate in the development of autonomous vehicles, manufacturers and this new category of suppliers will need to confront these issues directly and find mutually acceptable ways to allocate these risks throughout the supply chain. Doing so will require a team effort among engineers, business teams and lawyers because different technical solutions will provide different opportunities to mitigate risk through testing, contractual terms and insurance policies. In addition, the commercial terms will need to accommodate a far more iterative approach to developing detailed design specifications, which allows for the possibility that the initial allocation of responsibilities may change over time, as a result of testing, technology evolution and continued evolution of the still-developing regulatory framework.

In addition, manufacturers and suppliers must be prepared to assume and price-in risk over a much longer time period. The typical sourcing contract has a finite life, generally a five- to six-year term matching a typical vehicle model life, plus a commitment to provide replacement parts for another 10 or 15 years. Accordingly, while a traditional supplier may take full responsibility for the design and performance of its components, there is generally no duty to update that design or performance to account for evolving standards even over the production life of a particular model, and certainly no requirement to update vehicles already in the field. Agreements with information technology providers for add-on systems often have provisions regarding responsibilities for technology refresh and updates, taking into account the more iterative development cycle and need for periodic "bug" fixes. In the context of autonomous vehicles, even more ongoing collaboration and continued services between the manufacturer and supplier will be required.

NHTSA's recently issued guidance explicitly provides that the failure to update or upgrade software over the life of a vehicle may be considered a safety defect compelling a recall.[3] Commercial agreements for autonomous vehicle technology must allocate responsibility among the parties to track technology improvements and advances and implement them.

Conclusion

Contracting for vehicle equipment is becoming more complex with the growth of safety and cybersecurity risks and increasingly interconnected systems. The sourcing of technology and software to build connected and autonomous vehicles thus requires a diligent, thoughtful and creative approach to documenting contract requirements and specifications, allocating responsibilities and rights and adopting ongoing governance models to manage risks in this new landscape.

—By Marjorie H. Loeb and Linda L. Rhodes, Mayer Brown LLP

Marjorie Loeb is a partner in Mayer Brown's Chicago office and a member of the corporate and securities practice. Prior to joining Mayer Brown, Loeb was senior vice president and general counsel and secretary at Chrysler Group LLC. Linda Rhodes is a partner at Mayer Brown in Washington, D.C.

[1] NHTSA. (2016, September). Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Automated Safety Technologies, Docket No. NHTSA-2016-0040

[2] 49 U.S.C. 30101 et seq.

[3]See, NHTSA. (2016, September). Federal Automated Vehicles Policy: Accelerating the next revolution in roadway safety. Washington, D.C., which notes NHTSA’s expectation that for highly autonomous vehicles deployed on public roads, manufacturer’s will update software through over the air updates or otherwise.
