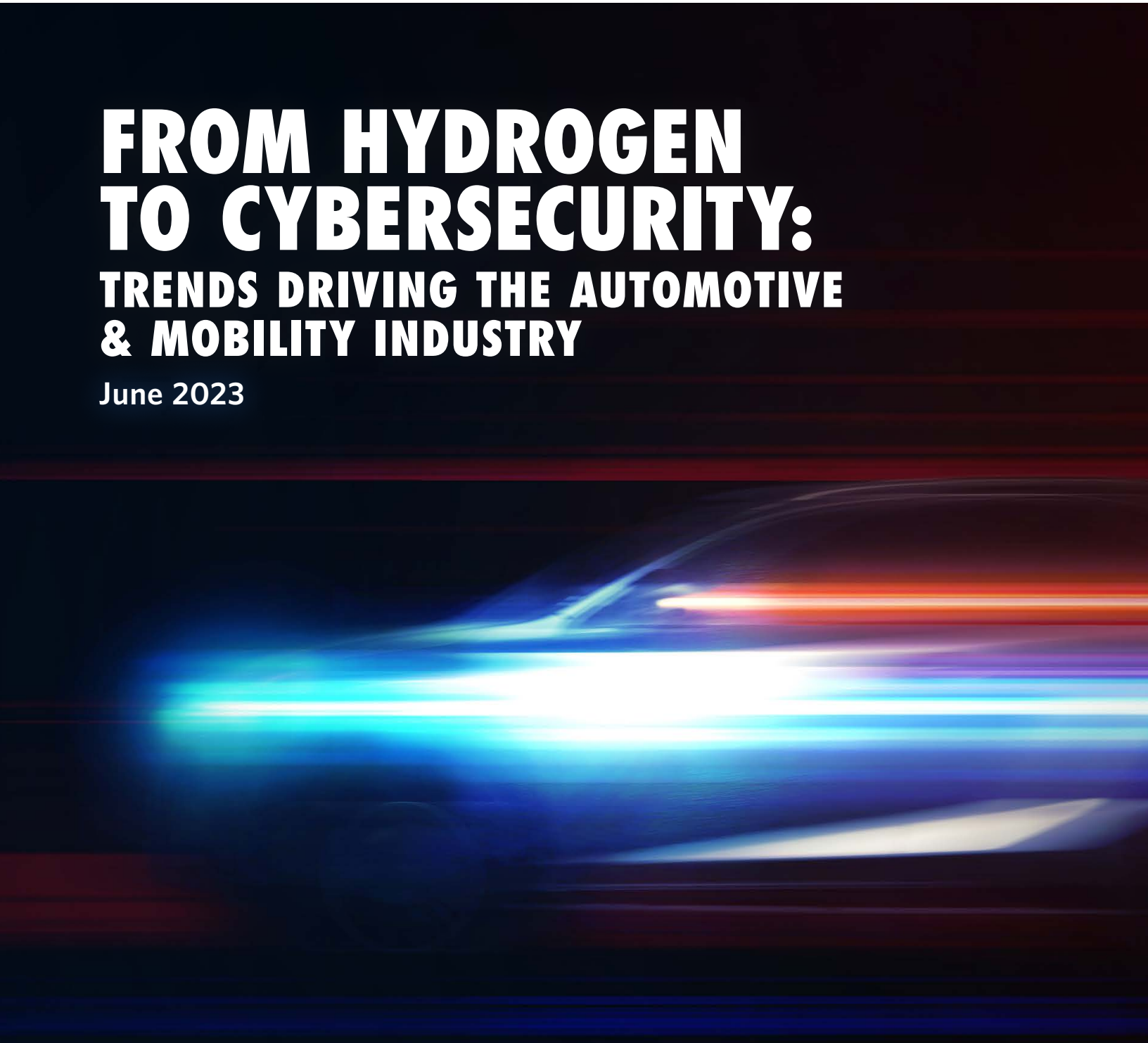
Morgan Lewis

REPORT

FROM HYDROGEN TO CYBERSECURITY:

TRENDS DRIVING THE AUTOMOTIVE & MOBILITY INDUSTRY

June 2023



www.morganlewis.com

Morgan Lewis

TABLE OF CONTENTS

FROM HYDROGEN TO CYBERSECURITY: TRENDS DRIVING THE AUTOMOTIVE & MOBILITY INDUSTRY

In May 2023, the Automotive & Mobility Industry Group at Morgan Lewis was invited to the State of Michigan by leaders of the Office of Future Mobility and Electrification for a series of meetings that provided unparalleled insights into the development of new technologies that will change how humans and goods are transported. As the birthplace of the personal mobility revolution, Michigan is committed to becoming the global leader for the incubation, and evolution of, autonomous, connected, electric, and alternative fuel technologies to better enable a clean energy future.

This report captures our thoughts on the most prominent opportunities that mobility stakeholders should aim to target and how to navigate the legal issues that must be considered when implementing these next-gen technologies. These include (1) electric vehicle (EV) and hydrogen fueling infrastructure; (2) cybersecurity and data privacy risks surrounding the EV ecosystem; and (3) the rollout of Level 2, 3, and 4 ADAS technologies in passenger vehicles and commercial trucks.

KEY LEGAL CONSIDERATIONS FOR ELECTRIC VEHICLE AND HYDROGEN FUELING INFRASTRUCTURE

Authors: Levi McAllister and Pamela T. Wu

Electric vehicles (EVs) and hydrogen fuel cell vehicles will be key players in the nationwide and industrywide effort to cut emissions. The industry has been focused on battery electrification for light-duty vehicles and the expansion of the EV charging infrastructure. Increasing attention is being paid to using hydrogen and adopting hydrogen fuel cell technologies in the heavy-duty transportation sector, as hydrogen is viewed as the option with the greatest long-term opportunity for decarbonizing that sector.

The Biden administration has made significant investments through grants and incentives to encourage and accelerate the development of the charging and fueling infrastructure and the continued development of hydrogen fuel cell technologies. The industry will need to consider and address a variety of commercial and legal issues to meet the ambitious greenhouse gas emissions reduction goals that the Biden administration has established for both types of transportation.

HYDROGEN USE IN THE HEAVY-DUTY TRANSPORTATION SECTOR

Alignment of the development and deployment of hydrogen fuel cell vehicles and the availability and accessibility of hydrogen fueling stations will be critical to the successful incorporation of hydrogen fuel cell vehicles into transportation fleets to decarbonize the heavy-duty transportation sector.

Operators of hydrogen fuel cell vehicles must have certainty that hydrogen fueling stations will be accessible and available along their travel routes. At the same time, investors and developers of hydrogen fueling stations need assurance that hydrogen fuel cell vehicles will be on the road and will refuel at their stations to justify their investment and development.

Scaling hydrogen fuel cell vehicles will require continued investment, research, development, and demonstration of hydrogen fuel cell technologies to enable the fuel cell durability, cost, and performance that is required for heavy-duty vehicle use.

The US Department of Energy has made available $47 million to fund the research, development, and demonstration of hydrogen carriers with unique storage and delivery methodologies, onboard storage of liquid hydrogen, and liquid hydrogen transfer and vehicular fueling technologies for medium- and heavy-duty applications. The department has also made available $750 million for, among other things, improving the efficiency, durability, and cost of producing clean hydrogen using electrolyzers. Additional funding to further these efforts is expected to be made available in the near future.

Significant expansion to the existing hydrogen fueling infrastructure is needed to successfully incorporate hydrogen fuel cell vehicles in heavy-duty transportation fleets. The hydrogen fueling stations that exist today are located predominantly in California, which limits the overall range and reach of hydrogen fuel cell vehicles in the United States.

Key issues for investors and developers of hydrogen fueling stations to keep front of mind as they continue their efforts to accommodate the expected increase in use of hydrogen fuel cell vehicles include the issues discussed below.

Source of the Hydrogen

The scope and design of a hydrogen fueling station is directly impacted by the production site of the hydrogen that is dispensed from the fueling station. If the hydrogen is delivered to the hydrogen fueling station, the hydrogen can be delivered to an onsite storage tank or delivered in a container that can be swapped out at the station. On the other hand, if the hydrogen is produced onsite, the station design will need to account for the necessary equipment and any feedstock needed for the production of hydrogen.

Purity of the Hydrogen

The hydrogen that is dispensed from the hydrogen fueling station will need to meet certain purity requirements for use in a hydrogen fuel cell vehicle. Hydrogen fuel quality testing may need to be performed to confirm the quality and purity of the dispensed hydrogen.

Access to the Hydrogen Fueling Station

The hydrogen fueling station must have dispensing equipment that is compatible with the hydrogen fuel cell vehicles the hydrogen fueling station may serve.

Ownership of the Hydrogen Fueling Station

A station owner may not always own the property on which the hydrogen fueling station is constructed. Depending on whether the station owner owns or leases the property, there may be restrictions or limitations on the permitted use of the property and the type of equipment and facilities that may be installed on the property.

Regulatory Uncertainty

There remains a lack of a comprehensive regulatory framework that applies to hydrogen and the infrastructure that is used to produce, transport, and store hydrogen in the United States. The Occupational Safety and Health Administration, Environmental Protection Agency, and Pipeline and Hazardous Materials Safety Administration currently exercise some form of regulation over hydrogen. However, other federal agencies, including the Federal Energy Regulatory Commission and Surface Transportation Board, may play a role in regulating hydrogen and the development of hydrogen infrastructure, although they have yet to do so.

EV CHARGING INFRASTRUCTURE

The Biden administration has long been focused on an expansive plan to promote the development and adoption of EVs. With an August 2021 announced goal for EVs to make up 50% of all vehicles sold in the United States by 2030, the administration has worked to propose or implement investment of $7.5 billion for building a national network of 500,000 EV chargers; tax incentives for buyers of new and used EVs; domestic production of the semiconductors, batteries, and minerals for EVs; and the most aggressive federal vehicle emissions standards to date.

Network charging infrastructure is a threshold issue to be addressed in order to get more EVs on the roads in US markets. Range anxiety, exacerbated by what many potential consumers view as inadequate EV charging opportunities throughout the United States, is considered to be an obstacle to the Biden administration's stated goal of achieving 50% zero-emission vehicles by 2030. Currently, the United States has approximately 140,000 public EV chargers. However, analysts project that the country will require approximately 1.5 million public EV chargers to meet the administration's 2030 goals.

Some of the most germane issues that EV market participants must consider relate to the following.

Commercially Successful Siting of EV Charging Infrastructure

Charge point operators or real estate owners will need advantageous site host agreements that address numerous issues to protect their rights and provide them monetary success in the arrangement. These agreements should consider elements such as

- Exclusivity in installation;
- Operations and maintenance responsibility;
- Revenue sharing and leasing payments;
- Ownership of property after termination; and
- Indemnification and insurance.

In addition, charge point operators must take care to consider the impact of utility rate design mechanisms and applicable usage patterns when modeling the extent to which energy sales opportunities can be commercially successful.

EV Infrastructure and Interconnected Utility Data Protection and Cybersecurity

Undeveloped cybersecurity and data protection standards and requirements for EV infrastructure could make consumer data vulnerable to hackers. This could also create entry points for hackers seeking to disrupt the US electric grid.

Vehicle-to-Grid Market Access, Monetization, and Regulatory Implications

Bidirectional charging allows EV customers or fleet lessors to use vehicle-to-grid capabilities to run power from the EV back into the grid, which can facilitate market access. However, vehicle-to-grid use may also trigger the need for energy services management functions between the EV operator and either its owner or the charge point operator. There are also regulatory implications of engaging in vehicle-to-grid activities by either the charge point operator or customer.

CYBERSECURITY CONSIDERATIONS FOR THE ELECTRIC VEHICLE ECOSYSTEM

Authors: *Levi McAllister and Arjun Prasad Ramadevanahalli*

US President Joseph Biden recently described our digital world as being at an "inflection point." Indeed, the rapid proliferation of new technology has created complex, and sometimes hidden, digital interdependencies that are vulnerable to exploitation, challenging the private sector and government to contain risks before they become unmanageable. It is no surprise that cybersecurity is now an essential component of modern business.

Whether it is securing customer payment data or guarding the nation's most critical infrastructure from state-sponsored hackers, companies across numerous industries are coming to terms with the importance of cybersecurity controls and accepting one undeniable truth—keeping up with the cyberthreat landscape is difficult but imperative. Each day, more components of daily life are becoming digitized and integrated with other digital systems, thereby presenting more necessity, complexity, and risk.

The confluence of digital systems in the electric vehicle (EV) industry is a perfect example of that phenomenon. Deploying EVs and EV supply equipment (EVSE), such as charging equipment, involves multiple interconnected platforms, connections to electric grid infrastructure, and exchanges of operational and customer data, all spread over a wide geographic footprint, presenting a target rich environment for threat actors.

For example, a large-scale compromise of grid-connected EVSE could cause electric distribution system disturbances by manipulating load patterns or system voltage. Threat actors could also introduce malicious software to a customer's EV by first compromising an unsecured charging station to which that EV eventually connects.

Data privacy risks are also present. The EV ecosystem involves many different exchanges of customer information, including personally identifiable information and payment information. Such data, whether stored locally on the EVSE or in a remote server, presents a valuable target for threat actors.

Data concerns are not just limited to foul play. Inadvertent data disclosures or larger breaches due to poor data management practices will invite scrutiny and legal liability. To address these risks, EV and EVSE companies will need to shore up cybersecurity risk management practices while keeping the following challenges in mind.

NOTABLE CHALLENGES

- *Regulatory Uncertainty*: While regulations are often accompanied by compliance and legal risks, they can also be useful for the private sector, as other industries have demonstrated. Mandatory requirements establish a baseline set of principles for the industry and drive accountability within regulated organizations. There are currently no mandatory cybersecurity requirements in place for the EV ecosystem. However, the federal government may be ready to change its approach. Earlier this year, the Biden administration released its National Cybersecurity Strategy, which concluded that mandatory cybersecurity requirements should be implemented for key critical infrastructure sectors because voluntary approaches have thus far been inadequate. While that call for regulation is currently just a policy declaration—and even so is not applicable to all

commercial EVs or EVSE—it is possible the federal government will continue exploring the need for additional legal authorities to make EV cybersecurity regulation a reality.

- *Evolving Data Privacy Laws*: As recent data privacy lawsuits in California and Illinois demonstrate, managing the appropriate use of customer data is becoming increasingly challenging. There is a patchwork of state-mandated privacy laws covering everything from Social Security numbers to biometric information. Adding to the challenge is the speed with which the legal landscape is changing. In the absence of a comprehensive federal data privacy framework, more and more states are enacting privacy legislation.

- *Secure by Design and Liability Risks*: In engineering parlance, "secure by design" means that a product is designed to be as foundationally secure from vulnerabilities as possible. Many products in the marketplace today are not designed with those principles in mind and are deployed with significant security vulnerabilities that can be exploited by threat actors. EV and EVSE manufacturers will need to pay particularly close attention to the cybersecurity risks across the entire lifecycle of a vehicle or a charging station (from conception to decommissioning) posed by items or software in their supply chains to avoid issues down the line.

RECOMMENDED STEPS

There are several key steps that EV and EVSE manufacturers can take today to limit their cybersecurity exposure and the attendant legal risk. **First**, EV and EVSE manufacturers should establish robust internal cybersecurity programs to identify and implement cybersecurity protections for vehicles and charging stations.

Those programs should use a risk-based approach to prioritize the most critical systems that pose the greatest risks to health and human safety. Cybersecurity programs should also have incident response plans that are designed to ensure recovery from cybersecurity incidents, robust cybersecurity awareness training, and procedures to encourage information sharing within relevant industry groups (for example, through the Automotive Information Sharing and Analysis Center or Auto-ISAC).

Second, in the absence of mandatory federal requirements, EV and EVSE manufacturers should carefully evaluate existing voluntary programs and guidance for cybersecurity risk management. For example, the US Department of Transportation's National Highway Traffic Safety Administration recently refreshed its Cybersecurity Best Practices for the Safety of Modern Vehicles.

The Federal Highway Administration also published a final rule establishing new minimum standards and regulatory requirements for light-duty EV chargers funded under the Infrastructure Investment and Jobs Act. Other standards-setting organizations have released cybersecurity frameworks specific to the EV industry, such as the International Organization for Standardization's ISO/SAE 21434:2021.

The National Institute for Standards and Technology is also developing a cybersecurity framework that will provides users with a national-level, risk-based approach for managing cybersecurity activities for EV extreme fast charging (XFC) infrastructure.

Third, EV and EVSE companies should implement supply chain risk management programs to evaluate critical commercial hardware and software components used in EVs and charging equipment. As most of those supply chain risks originate with vendors of products and services, supply chain risk management programs should address vendor risks at each stage of the procurement lifecycle—from initial identification of the vendor, to the installation of products or implementation of services, and finally

through the termination of the vendor relationship. EV and EVSE companies developing new programs can consider approaches taken in critical infrastructure sectors, such as the electric power industry, to identify, assess, and mitigate vendor risks.

Fourth, EV and EVSE organizations should foster a culture that prioritizes cybersecurity awareness. This includes elevating the risk management discussion to the highest levels within the organization and ensuring that key members have a seat at the table when addressing cybersecurity.

Additionally, EV and EVSE companies should regularly engage with government stakeholders when appropriate to do so, proactively participate in administrative rulemakings and notice and comment proceedings, and explore direct engagement opportunities with regulators. Ultimately, it is important to educate regulators to ensure that mandatory requirements, if implemented, are operationally and commercially viable for the regulated industry.

THE FIVE-YEAR OUTLOOK ON ADAS LEVEL 2, 3, AND 4 TECHNOLOGIES IN PASSENGER VEHICLES AND COMMERCIAL TRUCKS

Authors: *Daniel S. Savrin, F. Jackson Stoddard, and Mark J. Fanelli*

The prospect of autonomous vehicles whisking passengers and goods to their final destinations has dazzled the public's imagination and driven billions of dollars in investment into the development of advanced driver-assistance systems (ADAS) over the last decade. By 2035, market analysists project that ADAS technologies could yield $300 billion to $400 billion in revenue for legacy automakers and systems manufacturers.

Despite certain setbacks that have delayed the broad implementation of autonomous vehicles, leading mobility stakeholders remain committed to ADAS technology development and its potential to transform the future of transportation, from reducing the number of on-road accidents to increasing transportation logistics and supply chain efficiencies.

The ADAS technology investment strategy has shifted and appears likely to continue to do so. As legacy automakers undergo extensive restructuring to allow for the mass production of electric vehicles (EVs), ADAS technologies has become more focused on systems that can generate value for manufacturers in the next five years. In 2021, investors poured a record $9.7 billion into the development of ADAS technologies. In 2022, those investments dropped by almost 60% to $4.1 billion.

These smaller, more targeted investments are indicative that ADAS systems are maturing, and more legacy automakers are focused on bringing ADAS technology, but not fully autonomous vehicle technologies, to market based on consumer demand.

In light of these trends, we anticipate that additional Level 2 and 3 ADAS technologies will continue to be introduced in passenger vehicles at an increasing level over the next five years, while Level 4 ADAS technology capabilities are more likely to be a focus for commercial trucks. Below we detail the trends and developments that have brought us to this point and the issues and opportunities they present to auto industry stakeholders.

THE ROAD AHEAD: PASSENGER VEHICLES

Opportunity: Legacy automakers and mobility stakeholders will be introducing several new Level 2 and 3 ADAS technologies, which are designed to improve occupant safety and reduce accidents, in passenger vehicles, but the driver must remain ready to override the system and maintain control of the vehicle. Pursuant to SAE J3016, *Driving Automation Systems for On-Road Motor Vehicles* (more commonly known as the SAE Levels of Driving Automation), there are six levels of ADAS technologies, ranging from Level 0 (no driving automation) to Level 5 (full driving automation).

Level 2 ADAS include "partially automated" ADAS systems that combine automated functions, such as acceleration and steering, with the driver remaining fully engaged in the driving tasks at all times. Level 2 ADAS technologies require vehicles to be equipped with lidar systems that add materially to component costs, though some of the sensor and computing costs are decreasing.

Level 2 ADAS include features such as low-speed in-path object monitors, adaptive cruise control that can navigate regular traffic, heavy traffic jam pilots, and adaptive braking. It is expected that legacy

automakers and mobility stakeholders will continue to invest in Level 2 ADAS adoption while they continue developing more advanced autonomous systems.

Legal Considerations: Development of safety architecture and guidance are core components of ADAS systems development, including robust consumer-facing disclosures that explain that Level 2 ADAS technologies are not substitutes for relinquishing human control over the vehicle.

Opportunity: Level 3 ADAS include "conditionally automated" technologies, which still prioritize human driver control. With Level 3 ADAS, human drivers can transfer safety-critical functions to the ADAS under certain traffic and environmental conditions, such as light or moderate traffic or in clear, precipitationless weather.

This level of automation requires advanced sensor packages, hardware backups, and sophisticated software to keep occupants safe, which carry material added component costs for each vehicle. The maturation of Level 3 ADAS technologies over the previous four years, as well as consumer demand for them, has been deemed to warrant continued investment in the evolution of these systems for passenger vehicles.

Legal Considerations: In addition to the legal considerations involving Level 2 ADAS technologies and consumer education discussed above, as the autonomous capabilities of ADAS systems become more advanced and can assume conditional control of the vehicle for longer periods of time, manufacturers and investors of Level 3 ADAS should be cognizant of the need to develop and update the ADAS cybersecurity and data privacy safeguards.

Implementation of reasonable cybersecurity and data privacy practices are essential for a variety of reasons, including becoming a market leader in cybersecurity and data privacy that inspires additional investment and consumer confidence in products.

LEVEL 4 AND LEVEL 5 ADAS TECHNOLOGIES: IN IT FOR THE LONG HAUL

Opportunity: Because of the steep development and validation costs for Level 4 ADAS technologies, which are projected to potentially exceed $1 billion per system, it is more likely that Level 4 ADAS would be first considered and adopted for commercial use, primarily commercial truck use. Level 4 ADAS, or "high automation" technologies, are designed to perform all safety-critical driving functions and monitor roadway conditions for the entire trip.

Level 4 ADAS technologies are limited to the "operational design domain" of the vehicle. In other words, the ADAS is not designed to account for every driving scenario. Presently, Level 4 ADAS is the highest level of autonomous driving technology available. Level 5 ADAS technologies, which do not require human attention and eliminate the "dynamic driving task," are still in the conceptual stage. At the current rate of ADAS development, Level 5 ADAS technologies may not begin to appear as an option on US public roads for another 7 to 10 years.

Legal Considerations: Manufacturers and investors should be prepared to address the critical legal differences between autonomous vehicle standards in the United States and Europe, especially in light of the research and development costs associated with Level 4 and 5 ADAS technologies.

Level 4 ADAS technologies, installed in Class 4 to 8 trucks, could revolutionize the commercial trucking industry by reducing long-term costs and increasing supply chain efficiencies. During the COVID-19

pandemic, supply chain routes between seaports to rail depots and distribution centers ground to a halt due to labor shortages and caused bottlenecking in the consumer goods and manufacturing industries.

The pandemic highlighted the need for additional support for seaport to rail depots and distribution centers, among other trucking and shipping needs. Level 4 ADAS systems in commercial trucks could allow for 24/7 service on critical support routes. With respect to last-mile transportation, several parcel-delivery services have invested in Level 4 ADAS technologies that can support the delivery of goods from distribution centers and final purchasers.

Level 4 ADAS technologies are currently in use and in testing phases, and their on-road presence will likely continue to expand, particularly in states that have encouraged Level 4 ADAS development and deployment, such as Michigan, Arizona, Nevada, Texas, and Florida.

Level 4, and the future development of Level 5, ADAS technologies could eventually support the trucking industry. The Teamsters and other labor groups have been applying pressure on state legislatures to pass laws that would limit deployment of such ADAS technology by, for example, requiring at least one safety driver in the cabin of every semi- or fully autonomous commercial truck.

Legislation is pending in a number of states that may impede deployment of Level 4 or 5 ADAS technologies in the commercial trucking sector and, as such, while Level 4 ADAS technology in commercial trucks appears to be the way of the future, its deployment may remain state dependent, barring federal intercession (which appears to remain unlikely).

LEVELING UP: WHAT'S NEXT?

Because of the advancements in autonomous driving technologies, the next five years are critical for legacy automakers and mobility investors to capitalize on their investments and become market leaders in the Level 2, 3, and 4 ADAS technology segments. The shift in ADAS investment shows that certain stakeholders are satisfied with the development of their autonomous vehicle systems and will expand their product offerings that are supported by in-house research and development, albeit with the short-term focus for passenger cars and light trucks on Level 2 or 3 ADAS deployment while commercial vehicles are likely to be the primary focus for investment in, and deployment of, more advanced technology.

CONCLUSION

Opportunities and challenges continue to emerge in the ever-evolving automotive and mobility space, including developing hydrogen fuel infrastructure; safeguarding EVs, EV supply equipment, and the electrical grid from cyber threat actors; and introducing more complex ADAS technologies in passenger and commercial vehicles.

Morgan Lewis's Automotive & Mobility team offers unique insight into the complex legal and regulatory issues automakers, component manufacturers, technology suppliers, distributors, and other mobility stakeholders need to consider before pressing the pedal today on the trends that are driving the industry toward tomorrow.

CONTACTS

If you have any questions or would like more information on the issues discussed in this report, please contact any of the following:

Boston

Daniel S. Savrin	+1.617.951.8674	daniel.savrin@morganlewis.com
Noah J. Kaufman	+1.617.341.7590	noah.kaufman@morganlewis.com
Nathaniel P. Bruhn	+1.617.951.8651	nathaniel.bruhn@morganlewis.com

Philadelphia

R. Brendan Fee	+1.215.963.5136	brendan.fee@morganlewis.com
Mark J. Fanelli	+1.215.963.5069	mark.fanelli@morganlewis.com

Silicon Valley

Dion M. Bregman	+1.650.843.7519	dion.bregman@morganlewis.com
Rahul Kapoor	+1.650.843.7580	rahul.kapoor@morganlewis.com
Andrew J. Gray IV	+1.650.843.7575	andrew.gray@morganlewis.com

San Francisco

Brent A. Hawkins	+1.415.442.1449	brent.hawkins@morganlewis.com
F. Jackson Stoddard	+1.415.442.1153	fjackson.stoddard@morganlewis.com
Molly Moriarty Lane	+1.415.442.1333	molly.lane@morganlewis.com

Los Angeles

Lisa R. Weddle	+1.213.612.7334	lisa.weddle@morganlewis.com
David L. Schrader	+1.213.612.7370	david.schrader@morganlewis.com

Washington, DC

Levi McAllister	+1.202.739.5837	levi.mcallister@morganlewis.com
Pamela T. Wu	+1.202.739.5199	pamela.wu@morganlewis.com
Arjun Prasad Ramadevanahalli	+1.202.739.5913	arjun.ramadevanahalli@morganlewis.com
Timothy P. Lynch	+1.202.739.5263	timothy.lynch@morganlewis.com

New York

Robert W. Dickey	+1.212.309.6687	robert.dickey@morganlewis.com

Chicago

Elizabeth B. Herrington	+1.312.324.1445	beth.herrington@morganlewis.com
Stephanie L. Sweitzer	+1.312.324.1741	stephanie.sweitzer@morganlewis.com
Philip W. Russell	+1.312.324.1743	philip.russell@morganlewis.com

Brussels

Christina Renner	+32.2.507.7524	christina.renner@morganlewis.com

Frankfurt

Michael Masling	+49.69.714.00.753	michael.masling@morganlewis.com

Shanghai

Todd Liao	+86.21.8022.8799	todd.liao@morganlewis.com

ABOUT US

Morgan Lewis is recognized for exceptional client service, legal innovation, and commitment to its communities. Our global depth reaches across North America, Asia, Europe, and the Middle East with the collaboration of more than 2,200 lawyers and specialists who provide elite legal services across industry sectors for multinational corporations to startups around the world. For more information about us, please visit www.morganlewis.com.