DICKINSON WRIGHT

PLUGGED IN

AN EV NEWSLETTER

Volume 2, Number 9

You’re Invited! Please find details and an agenda enclosed.

The Convergence of Electrification and AI

An Evolving and Uncharted Business and Legal Landscape

Tuesday, November 19, 2024, 3:30 – 7:30

MSU Executive Education Center
811 West Square Lake Road, Troy, Michigan

CLICK TO REGISTER

Editor’s Note

November’s edition of *Plugged In* concludes a three-part series focused on the impact of technology and AI on the automotive industry. DW Member Greg Ewing discusses the significant cybersecurity and privacy risks associated with connected cars, vehicles equipped with built-in internet connectivity. As cars become increasingly connected, they generate vast amounts of data, raising significant cybersecurity and privacy concerns. Greg’s article explores the potential risks of connected vehicles, from hacking vulnerabilities to data privacy issues, and outlines how automakers and consumers can protect themselves in this rapidly evolving landscape. Next, Bob Weiss considers the contrasting perspectives on Tesla’s future in the autonomous driving industry, with some voicing optimism about the company's potential to dominate the space while others express skepticism about regulatory, technological, and competitive challenges. The newsletter concludes with Bob’s interview of Doug Patton, Principal of Jupiter Consulting LLC and a former automotive industry executive. The interview covers a range of topics, including battery technologies, the symbiotic relationship between electrification and autonomous driving, the current technological competition between Tesla and Waymo, and global EV market challenges, including China's growing dominance.

Heather Frayre | Member Partner

Dickinson Wright

AUTOMOTIVE INDUSTRY ELECTRIFICATION & AI

The Convergence of Electrification and AI

An Evolving and Uncharted Business and Legal Landscape

Tuesday, November 19, 2024, 3:30 – 7:30

MSU Executive Education Center

811 West Square Lake Road, Troy, Michigan

The global automotive industry embarked on a rapid and unprecedented transformation in its race to EVs. Although the electrification pace has slowed in the U.S., total electrification seems inevitable. AI's rapid rise is already affecting the electrification transformation, and its ultimate effect is likely to be significant.

As the convergence of AI and EVs accelerates, that will create stress on automotive suppliers and require new legal paradigms to address the significant legal issues this convergence raises.

We are excited for you to join us on November 19, 2024 for two complimentary, fast-paced, panel-discussions of the business and legal issues arising in the race to electrification and AI. Topics include:

- An update from Steve Wybo of Riveron on the health of automotive suppliers and how that impacts electrification and AI.
- Moral and legal Issues implicated in AI decision making.
- Uncharted and developing legal-liability issues.
- Cybersecurity considerations.
- Privacy and regulatory considerations.

A cocktail reception will follow immediately after the panel discussions.

CLICK TO REGISTER

To register, please click the registration button.

Please note that registration is limited. We look forward to seeing you.

The Far Reaching Cybersecurity and Privacy Impacts of Connected Cars

Imagine a company that can pinpoint the exact location of every car in the world or data about all of your driving habits and routes being used to identify your friends and family, to recalculate your health insurance, or to send advertisements for the coffee shop on your way to your kid's school. All of this is possible – if not already happening – with our connected cars. The wealth of data generated by our connected cars raises incredibly significant cybersecurity and privacy concerns that must be addressed.

1. What is a Connected Car?

A connected car is any car – electric, hybrid, or gas powered – with a built-in cellular modem that allows that car to communicate over the internet. These cars generally come with a service to manage that communication. Chevrolet and General Motors have OnStar. Ford has FordPass. Stellantis has Uconnect. Many vehicles allow consumers to bring their own with Android Auto or Apple Car Play. In 2020, 91% of new cars sold in the U.S. were connected.[1] The percentage of new US vehicles that will be connected is predicted to hit 95% by 2030.[2]

This connectedness provides a myriad of new features and conveniences. Our navigation systems tell us where to go, our telematics systems track our operation of the vehicle and notify us of needed service, and our infotainment systems keep us entertained while we drive or wait.

But now, by adding signals in and out, we've added significant potential threat vectors and new areas for potential invasion of privacy. In the past, an attack on a car was generally mechanical: breaking a window, picking a lock, hotwiring the ignition. Our connected cars provide many more opportunities for attack.

2. Five functional areas lead the cybersecurity and privacy concerns.

There are at least five primary functional areas of concern with our connected cars. First, telematics systems use sensors to track the location and operation of a vehicle. This data is often shared through the OEM so that consumers can manage the vehicle. This may include remotely starting the vehicle, calling emergency services in case of an accident, remotely setting climate controls, opening windows, or starting and stopping music. Many third-party apps allow these

[1] The Connected Car Market Will Endure a 15% Shipment Decline, Flat Revenues in 2020; Sales Return on Trend Early 2022 (available at https://www.prnewswire.com/news-releases/the-connected-car-market-will-endure-a-15-shipment-decline-flat-revenues-in-2020-sales-return-on-trend-early-2022-301100761.html).

[2] The Continuing Evolution of Automotive Cyber Security, IEEE Innovation at Work (available at https://innovationatwork.ieee.org/the-continuing-evolution-of-automotive-cyber-security/)

features and more. OEMs may use the same data to improve performance, identify problems early, or troubleshoot problems that arise.

Second, power-related systems generate voluminous data including information on remaining charge, distance available, time to refuel, etc. These in turn send data to OEMs or third parties to, for example, recommend the next charging or fueling location.

Third, navigation systems tell us how to get where we want to go and often include saved locations and favorite routes. But these systems also necessarily hold data on driving behavior, food preferences, family information, which doctors we visit, which events we attend, and other derivative data.

Fourth, infotainment systems store music choices. But potentially more importantly, store the consumer's voice and related voice commands, frequent numbers for calls and texts, potentially the actual content of calls and texts.

Fifth, there are numerous third-party apps such as Android Auto or Apple Car Play that can have access to any of the data above if the consumer agrees. Not only are these a distinct opportunity to access a vehicle, but they also invariably result in third-party databases storing large amounts of consumer data.

3. Why does any of this matter?

Why does this matter from a cybersecurity and privacy perspective? In 2019, an ethical hacker gained access to digital keys of cars worldwide for multiple different manufacturers. Then, using a third-party software package, the hacker executed commands on those cars – unlocked doors, opened windows, disabled security – without the driver's knowledge. The third party software provider fixed the problem.

Similarly, hackers gained access to data held by a device independent telematics company and were able to execute commands (unlock doors, start engines, honk horns) on consumer cars, police cars, ambulances, and other law enforcement vehicles.

As another example, in 2022, hackers gained access to vehicles and the ability to remotely start, unlock, locate, flash the lights, and honk the horn on the cars through a SiriusXM vulnerability. This system was used in cars made by Acura, BMW, Honda, Infiniti, Jaguar, Land Rover, Lexus, Nissan, Subaru, and Toyota.

Finally, in 2021, news broke of Ulysses, a third party that claimed to be able to give the military real time location data for 15 billion vehicles around the world.[3] It was able to provide this precise location information based on data collected by the cars and their components; they required no additional apps or access.

4. Companies can and should protect themselves and their customers.

In the face of consumer demand for connected features and the increased risk that these features bring, companies must protect themselves both to avoid a breach and, if it happens, after a breach.

One key way to protect both before and after a breach is to ensure that any connected vehicle or components of those vehicles apply well-regarded technical standards. There are numerous standards promulgated by many different organizations that apply to every aspect of connected vehicles. For example, Society of Automotive Engineers International (SAE),[4] International Standard of Organization (ISO),[5] Auto-ISAC, National Highway Traffic Safety Administration (NHTSA),[6] Cybersecurity Infrastructure Security Agency (CISA), NIST, and industry associations.

Applying these standards ensures a company is applying industry best-practices and therefore reduces its risk profile. Additionally, if an OEM or manufacturer does suffer a breach, it will most likely be judged in litigation, government investigations, and in the court of public opinion. In each of these fora, a company that applied industry standards pre-breach can point to those practices as proof that it took all reasonable precautions and protected its customers.

The NHTSA has also proposed an industry wide set of cybersecurity best practices for connected vehicles. Most notably, NHTSA encouraged the industry to create a mechanism for data sharing, Auto-ISAC.[7] Through Auto-ISAC, the industry is intended to find methods for accelerating the adoption of lessons learned across the industry, including effective information sharing before and after breaches.

5. Privacy considerations with connected cars are very high.

In addition to the cybersecurity risks related to accessing or controlling a vehicle without the owner's permission, connected vehicles raise numerous potential privacy concerns. Multiple

[3] Cars Have Your Location. This Spy Firm Wants to Sell It to the U.S. Military, Cox, Joseph, Vice.com (Mar. 17, 2021) (available at https://www.vice.com/en/article/car-location-data-telematics-us-military-ulysses-group/)

[4] Vehicle Cybersecurity Systems Engineering Committee (available at https://standardsworks.sae.org/standards-committees/vehicle-cybersecurity-systems-engineering-committee#)

[5] Road vehicles — Cybersecurity engineering (available at https://www.iso.org/standard/70918.html)

[6] Cybersecurity Best Practices for the Safety of Modern Vehicles (Sept. 2022) (available at https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf)

[7] Auto-ISAC (available at https://automotiveisac.com/).

privacy laws may apply to any data processing done by a connected car depending on what types of data are collected, who the data subjects are, and where the data is stored. For example, in the United States, this would include state privacy laws and Federal oversight provided by the FTC that ensures fair trade practices through transparency. In Europe, the United Kingdom, or Switzerland, the applicable version of GDPR will apply. In China, the Personal Information Protection Law (PIPL) and the Data Security Law (DSL) may be applicable.

To comply with the various privacy legal requirements, OEMs will generally be required to disclose the data collected by their vehicles, including data from any components incorporated in that car, how that data is used, and allow consumers to exercise their applicable rights. Similarly, if a connected vehicle collects biometric data such as voice, fingerprints, or facial images, the OEM will be required to meet the specific requirements of the relevant biometrics law. Failure to comply with these jurisdiction specific requirements could result in fines or sanctions from government authorities.

Consumers must also be aware that automakers may share biometric data – or other collected data – with law enforcement. The legal requirements to share with law enforcement may also be a lower threshold than most consumers expect. For example, the privacy policies covering this data routinely do not require police to provide a warrant, but instead indicate that data may be shared as "part of an investigation or request, whether formal or informal, from law enforcement or a governmental authority."

Over time there is no question that better and better security will be developed and privacy practices will be implemented. Simultaneously, bad actors will constantly strive to invent new ways to circumvent security and the volume of data will make data sharing with third parties more and more valuable. This is the typical ebb and flow of security and privacy but one which all drivers of connected cars should be aware.

Gregory L. Ewing | Member Partner

Tesla's Trajectory – A Matter of Significant Debate

There seem to be differing perspectives about the future of Tesla. In early October, in a major event, Tesla, or perhaps more particularly, its controversial Chief Executive Officer and majority owner, Elon Musk, unveiled two new vehicles: (1) the Cybercab, an autonomous driving vehicle with no steering wheel or pedals (projected cost of less than $30,000); and (2) the Robovan, an AV capable of transporting 20 occupants and cargo. Musk also touted Tesla's "Fully Self Driving" software. There are those who suggest that these and related autonomous driving products/services could increase Tesla's enterprise value to three trillion by 2030. Many analysts were lukewarm to the presentation, suggesting that given the lack of specifics in terms of timing, specific business model, etc., that there was more sizzle than steak to the presentation and that there were major unaddressed obstacles to Tesla achieving major success in autonomous driving.

On the other hand, there are those that embrace Musk's aggressive vision and believe that Tesla will succeed in being a leader in, if not ultimately dominate, the autonomous driving space and AI and their various applications.

Perhaps acknowledging the substantial lead its well-funded competitors have achieved in terms of experience and technology, an analyst from Oppenheimer poses the question this way: "The question we are left with is whether Tesla can leverage its significant data collection and manufacturing cost advantages into a dominant position in self-driving vehicles/services".

I will try to lay out both sides below (not exhaustively, given space limitations) and leave it to the reader to draw their own conclusion.

Pro Case

One of Tesla's biggest boosters is ARK, which has, as of September 30, 2024, approximately 5.6 billion dollars under management and describes itself as "a global asset manager specializing in thematic investing in disruptive innovation" headed by Kathy Wood. Tesla represents ARK's largest holding and constitutes approximately 15% of its portfolio. In a recent investment report entitled "Countdown to Cybercar, Tesla's Multi-Trillion Dollar Robotaxi Opportunity"[8], the author states: "In our view, an autonomous taxi platform will unlock a multi-trillion dollar market and begin to dominate Tesla's valuation approaching 90% of its enterprise value over the next five years." and projects a $2,000 stock price in 2027. On November 1, 2024, Tesla closed trading at $248.98 per share. ARK sees Robotaxi contributing 64% and EVs contributing 46% of Tesla's EBITDA in 2027.

[8] https://www.ark-invest.com/articles/analyst-research/countdown-to-cybercab

In its annual research report, entitled "Big Ideas 2024"[9], it notes that according to its research, ARK believes that robotaxi platforms could redefine personal mobility and generate $28 trillion in enterprise value during the next five to ten years.

ARK is not the only prominent Wall Street analyst that is very bullish on Tesla. Dan Ives of Wedbush Securities opines that he believes autonomous driving could be a trillion dollar opportunity for Tesla and said that he thinks Tesla is the most undervalued AI stock in the entire stock market. Analysts at Deutsche Bank are also optimistic regarding Tesla's prospects in autonomous driving, projecting an additional $4 billion in sales and an additional $1 billion in pretax earnings by 2030.

ARK, in its report noted above, addresses the issue of Tesla's competitors having entered into the AV market well before Tesla. The author notes that Tesla will scale faster than Waymo because it won't rely on HD maps or geofencing, but will use real world driving miles. Tesla customers drive 5 million miles per day in Full Self Driving (FSD) mode and 87 million miles per day in U.S. non-FSD, creating a database much larger and more diverse than Waymo. He further cited Tesla's U.S. based manufacturing capacity as an additional advantage that will allow Tesla to scale up rapidly and close the current lead-time gap with its prime competitor, Waymo, which currently has no manufacturing capacity of its own.

Acknowledging that autonomous driving, rather than sales of EVs, is the future of the company, Musk is quoted as telling investors that, "If somebody doesn't believe Tesla is going to solve autonomy, I think they should not be an investor in the company".

Cons

1. Regulatory Approval – One of the major obstacles to Tesla's entry into the autonomous driving field, let alone dominance, is regulatory obstacles. Although Tesla has driving testing permits that allows it to test autonomous technology with a safety driver on public roads, it does not have driverless testing permits, nor have they even applied for such permits according to *TechCrunch*, quoting a public information officer from the California DMV. Waymo has obtained regulatory approval and operates a Level 4 driving system in several cities. There are also federal regulatory requirements. As *TechCrunch* noted in a recent article, "If Tesla wants to mass produce its robotaxis with no traditional driver controls, it needs to obtain an exemption from the Federal Motor Vehicle Safety Standards" and that NHTSA has confirmed that Tesla has not applied for such an exemption, which will likely not be easy to obtain.

[9] https://www.ark-invest.com/big-ideas-2024

2. Its Competitors Are Way Ahead – In an article[10] appearing in the October 15th edition of Fortune, the author noted: "….by the time Tesla revealed its robotaxi vehicle on controlled private property, competitors have been out on the public roads in high-traffic, complex, urban areas for years." The author cites, in particular, Alphabet-owned Waymo, which is reported to conduct 100,000 paid rides a week in San Francisco and LA and is continuing to expand its operations to other major cities.

3. Technology – In an article appearing in the October 11th edition of the *Wall Street Journal* entitled: "Musk Shows Off Driverless Robotaxi to Be Priced Under $30,000"[11], the author notes how Tesla lags its rivals in terms of the state of its driverless technology stating, "Tesla also needs to make leaps in advancing its own driver-assist software, which today is considered a 'level 2' system (requiring some level of driver involvement)" and that, "By contrast, Waymo has achieved 'level 4' autonomy on its cars, which means it can operate them without a human driver in most circumstances."

There is another risk regarding Tesla's chosen technology. In an article entitled, "Have AI advances led to self-driving breakthroughs or a dead end"[12], the author highlights the risk related to Tesla's controversial choice of self-driving technology. In contrast to Waymo, Mobileye and others, Tesla had adopted "end-to-end" learning model, which is described as "ingesting tribes of data and produce driving commands without intermediate coded guardrails or insight into how results are derived." Waymo, on the other hand, has adopted what is described as more of a compound system that includes multiple components. Sterling Anderson, currently chief product officer of Aurora innovation and formerly chief of Tesla Autopilot, believes that Tesla's approach is "exactly wrong" and amounts to a "train and pray" strategy that provides no assurance of safe results or ability to vet a problem.

The *New York Times* and Bloomberg Law reported recently that NHTSA recently opened a defect investigation into Tesla's FSD, following reports of four crashes, one involving a fatality, while the system was in operation. In the October 18th *New York Times* article entitled, "Tesla Self-Driving System Will Be Investigated by Safety Agency"[13], the author noted that the focus of the investigation was whether Tesla's self-driving software had safeguards in place to require drivers

[10] https://fortune.com/2024/10/14/elon-musk-cybercab-robotaxi-visionlikely-several-years-away/

[11] https://www.wsj.com/business/autos/elon-musk-tesla-robotaxi-acfc5e3b

[12] https://www.reddit.com/r/SelfDrivingCarsNotes/comments/1g6nezc/have_ai_advances_led_to_selfdriving_breakthroughs/

[13] https://www.nytimes.com/2024/10/18/business/tesla-self-driving-investigation.html

to retake control of their cars in situations the autonomous technology couldn't handle on its own. The author concluded: "But the investigation by the safety agency is an indication that, even if Tesla succeeds in perfecting the technology, it will still face significant regulatory hurdles." The author further notes that "Tesla's self-driving software depends on cameras to operate, unlike other manufacturers who also use radar or laser technology that are often better at detecting objects and people when the view is obstructed by poor weather or bright sunshine."

Conclusion

There are plenty of what appear to be valid arguments on both sides of the debate. Perhaps the deciding factor might be Musk himself. Putting politics and personality aside, Musk is a driven genius and has a proven successful track record of proving his doubters wrong.

Robert Weiss | Of Counsel | Co-Chair, EV Initiative

Interview with Doug Patton of Jupiter Consulting LLC
October 23, 2024

Thanks so much for agreeing to sit down with me to discuss this very volatile time in the auto industry as the industry transitions to all EV product offerings.

Question 1

Bob: Tell us a little about your background and what you have been up to lately.

Doug: I am currently providing consulting services to the auto industry through my consulting firm, Jupiter Consulting LLC (www.JupiterConsultingLLC.com), focusing on electrification, automation and connectivity. Prior to that, I spent more than 30 years at Denso (one of the largest automotive suppliers in the world) and retired as North American Chief Technology Officer and Executive Vice President of Engineering. I have been active in SAE over the years and served as its president, as well as, president of the Detroit Engineering Society. In addition to my consulting, I am engaged in a start-up competition called GAMIC.

Question 2

Bob: Tell us a little about GAMIC.

Doug: GAMIC's mission is to accelerate early stage automotive and mobility start-ups to network, meet new partners, showcase their technologies and compete for rapid commercialization assistance through an annual competition. It gives the participants great opportunities to be mentored by and network with thousands of industry segments, engineers, executives, investors, etc. It is run by a group of former auto execs like myself. This is the 18th year of the competition.

Bob: Sounds fascinating. We will include a link to its website: https://gamicevent.org/

Question 3

Bob: So let's talk batteries for a few minutes. Today, the most common battery is the lithium ion battery. Do you see viable alternatives and, if so, given lithium's dominance and the enormous investment made in that technology, will it be feasible to adopt an alternative material?

Doug: First, I would note that there is still significant room to grow in advancing lithium ion batteries and there is a real focus on that process today by OEMs and suppliers. However, there are alternative technologies that are being worked on, as well. For example, sodium ion and solid state batteries. Sodium has the obvious benefits of ready availability and low cost.

Regarding the second part of your question, I do think that there is room to explore and if appropriate, adapt other technologies. The reason I believe that is that there isn't tremendous investment required to switch technology from a manufacturing perspective. You can use much of the same basic manufacturing technology and equipment that is currently being used for lithium for sodium and potentially other materials. It would take some adjustment; but nothing prohibitive from a time and cost perspective.

Solid state batteries are another promising technology. These have higher energy density and are not as susceptible to fires as conventional lithium ion batteries. The current challenge here is scale production.

Question 4

Bob: With all the advantages of sodium, why isn't it more in use?

Doug: Sodium has a number of technical challenges that have to be resolved, such as cycling; but over time those challenges are being overcome. It's been reported that CATL, one of the world's leading battery manufacturers, is introducing a sodium ion hybrid-battery that will have 250 miles range, 4C charging capacity and is unaffected by cold weather charging. By the way, it's also been reported that Stellantis is experimenting with solid state battery technology.

Regarding lithium and other technologies, improvements in weight, efficiency, and cost are inevitable. By analogy, look at the internal combustion engine. Over its lifetime there have been continuous incremental improvements from its earliest versions. The same will be true for battery technology and other aspects of electrification.

Question 5

Bob: Let's segue to the broader topics of electrification and autonomous driving. It seems like a year ago the media focus was electrification (battery technologies, infrastructure issues, range anxiety, slowing sales, hybrid competition, slowing EV sales, etc.), with little attention to autonomous driving. Today, the topic of autonomous driving and AI is what is all over industry and mainstream media. Does that reflect the reality of the industry's focus or just what the media decides to emphasize?

Doug: I agree with your perception of the media's emphasis; but I don't think it necessarily reflects the state of the industry. The industry remains focused on electrification, though consumer reluctance has slowed things down somewhat; but that is a temporary condition. Universal electrification is coming and the only open issues are timing and who the winners and losers will be.

With accelerating operations and expansion by Waymo, Cruise and others, and Elon Musk's big roll out of the Cybercab and the general infatuation with AI, media attention has shifted to autonomy and its intersection with AI. Let's face it, all aspects of society are being, or will shortly, be transformed by AI so that is what will be followed and perhaps exaggerated by the media. That emphasis will ebb and flow as electrification and autonomy evolve.

Question 6

Bob: Is there an intersection between electrification and autonomy? Stated otherwise, are their respective development intertwined or codependent?

Doug: Although they are separate in many ways, I believe they have in some sense, a symbiotic relationship. For example, the available power generated by the car’s battery has to be shared or perhaps allocated between powering the propulsion of the vehicle and the other features using AI, which we know requires significant power resources. So on the one hand they compete for power, but on the other hand AI creates efficiency, which reduces the need for power. For example, with the benefit of autonomous technology the vehicle can select a route that is more direct, less traffic, less hills, etc., thereby conserving energy. So to sum up, I would say they are very intertwined by the fact that both aspects require power and there is only one source of that power and that is the battery. So automation is part of the problem in that it demands power to function; but it is also part of the solution because it brings greater efficiency, which lessens the need for power.

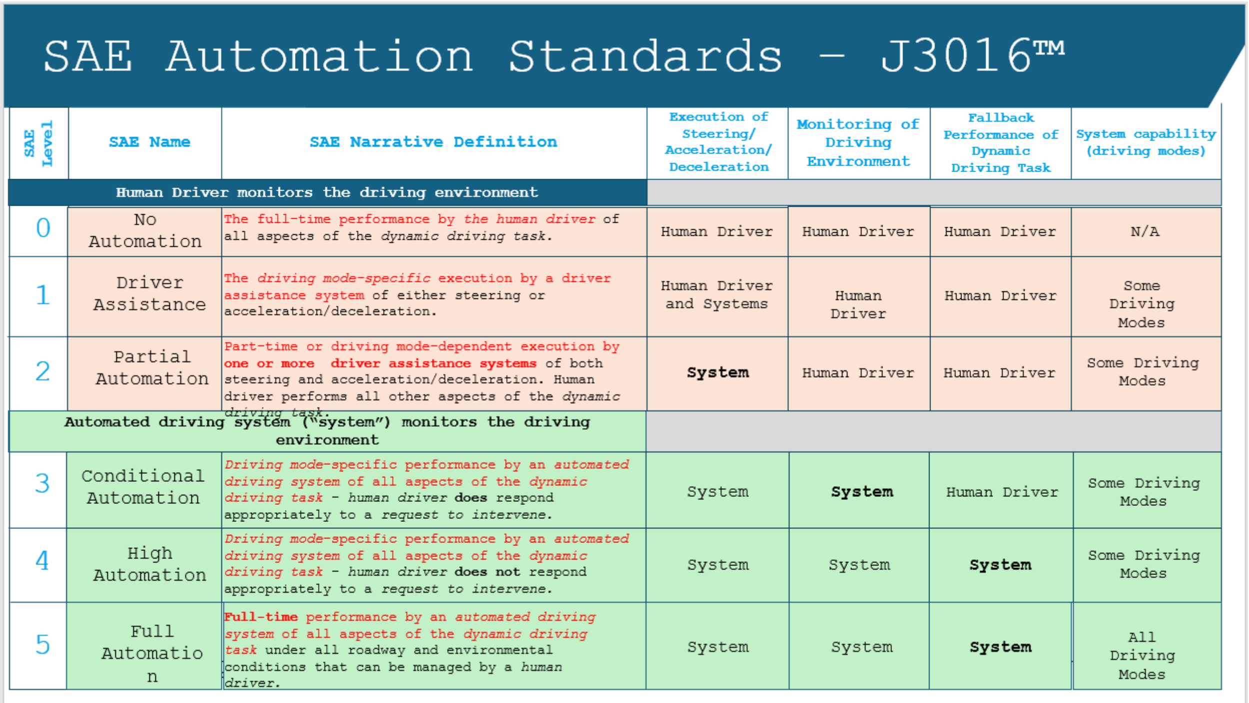
Question 7

Bob: So, before we delve much further into the realm of autonomous driving perhaps a tutorial of the basics would be helpful to put the state of that segment of the industry in perspective for our readers. My understanding is that there are 5 levels of autonomy. Would you define them and generally explain what levels need to be attained before it can be commercialized, and where the main players are today regarding the level of attainment?

Doug: There are 5 levels. Level 5 is no driver and passenger snoozing in the back seat. No human intervention in or outside of the vehicle. There are currently, to my knowledge, no companies offering Level 5 autonomous driving.

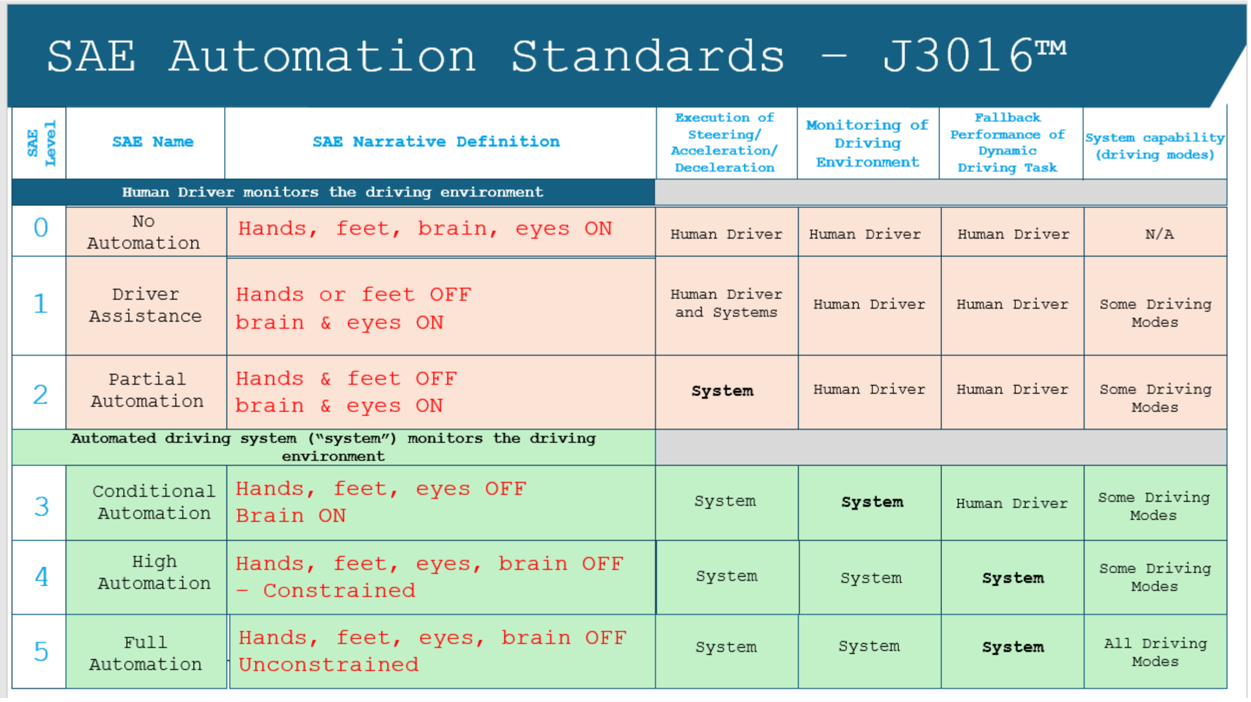
Level 4 requires some involvement by the person in the vehicle. Level 3 – You can have your hands off the steering wheel; but you have to be in a position to take over if the vehicle has a situation that it doesn't understand. The driver doesn't have to be constantly physically monitoring, but if prompted he/she can takeover. Level 2 – has to be watching the road and prepared to take over if necessary.

The SAE has developed automation standards and has prepared a chart which lists the 5 levels and their respective attributes, which I include below.



SAE Automation Standards – J3016™

SAE Level	SAE Name	SAE Narrative Definition	Execution of Steering/ Acceleration/ Deceleration	Monitoring of Driving Environment	Fallback Performance of Dynamic Driving Task	System capability (driving modes)
Human Driver monitors the driving environment						
0	No Automation	The full-time performance by *the human driver* of all aspects of the *dynamic driving task*.	Human Driver	Human Driver	Human Driver	N/A
1	Driver Assistance	The *driving mode-specific* execution by a driver assistance system of either steering or acceleration/deceleration.	Human Driver and Systems	Human Driver	Human Driver	Some Driving Modes
2	Partial Automation	Part-time or driving mode-dependent execution by **one or more driver assistance systems** of both steering and acceleration/deceleration. Human driver performs all other aspects of the *dynamic driving task*.	**System**	Human Driver	Human Driver	Some Driving Modes
Automated driving system ("system") monitors the driving environment						
3	Conditional Automation	*Driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task* - *human driver* **does** respond appropriately to a *request to intervene*.	System	**System**	Human Driver	Some Driving Modes
4	High Automation	*Driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task* - *human driver* **does not** respond appropriately to a *request to intervene*.	System	System	**System**	Some Driving Modes
5	Full Automatio n	**Full-time** performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*.	System	System	**System**	All Driving Modes



SAE Automation Standards – J3016™

SAE Level	SAE Name	SAE Narrative Definition	Execution of Steering/ Acceleration/ Deceleration	Monitoring of Driving Environment	Fallback Performance of Dynamic Driving Task	System capability (driving modes)
Human Driver monitors the driving environment						
0	No Automation	Hands, feet, brain, eyes ON	Human Driver	Human Driver	Human Driver	N/A
1	Driver Assistance	Hands or feet OFF brain & eyes ON	Human Driver and Systems	Human Driver	Human Driver	Some Driving Modes
2	Partial Automation	Hands & feet OFF brain & eyes ON	**System**	Human Driver	Human Driver	Some Driving Modes
Automated driving system ("system") monitors the driving environment						
3	Conditional Automation	Hands, feet, eyes OFF Brain ON	System	**System**	Human Driver	Some Driving Modes
4	High Automation	Hands, feet, eyes, brain OFF – Constrained	System	System	**System**	Some Driving Modes
5	Full Automation	Hands, feet, eyes, brain OFF Unconstrained	System	System	**System**	All Driving Modes

Question 8

Bob: How would you compare where Tesla and Waymo are respectively in terms of reaching level 4?

Doug: They each have advantages and drawbacks versus one another. For example, Waymo's robotaxi has been operating for a number of years in a commercial context with routes in San Francisco and LA and therefore has actual operating experience. On the other hand, its experience and data collection is limited to very specified (geofenced) and, in some ways, similar geographic areas (weather managed). On the other hand, Tesla does not have commercial operating experience; but has collected millions of miles of data on all types of conditions and topography. The managed conditions of Waymo allow for level 4 operations within those defined areas, but arguably not beyond.

Question 9

Bob: Do Waymo and Tesla use the same basic technology?

Doug: No, they are very different. Waymo uses a LiDAR system of sensors, while Tesla uses a camera based technology. In my view, Tesla's technology is inferior because it relies only on cameras as opposed to different sensors, which have different capabilities in different situations. For long range front of the vehicle perspective, you need LiDAR. Also, it is reported that Tesla has no internal guardrails. By that I mean, it's just letting the vehicle make its own decisions based on the data that has been programmed as opposed to programmed safety parameters. By guardrails, I mean that there are some overarching principles embedded in the system that will guide the vehicle how to react in certain safety related situations, i.e., given the data I have, how do I react? Tesla will ultimately make it work; but the real question is to what degree? Will it be effective for 99.9% of the situations or 98.9%? The question is does that 1 or 2% make a difference to regulators, to the consumers or to the legal system?

Question 10

Bob: Shifting to the current slow-down of EV sales, the OEMs are reacting by implementing heavy discounts and favorable leases, is there anything that the OEMs can do to stimulate sales?

Doug: For one thing, I think the dealers can do a lot more in attempting to understand the specific needs of the customers and then with that information educating the customer regarding the specific model EV's capabilities that would be consistent with the specific driving requirement. It won't always result in selling an EV; but it will result in a more satisfied customer and perhaps gradual openness to explore an EV option.

Question 11

Bob: Finally, no interview would be complete these days without a discussion of China's growing dominance in the EV space. Much has been written about China's advancements in EV technology, engineering, styling, cost structure and extraordinary government support. Can the rest of the world's manufacturers be competitive?

Doug: It's possible; but it is going to be very difficult. It is going to require some kind of significant technological breakthrough, whether the technology used in the vehicle itself or in the manufacturing process, either of which is possible. However, the Chinese are investing massively in advancing their own technology so they will likely equal or excel at further technological advancements and thereby maintain their competitive advantage.

Bob: Doug, thanks so much for your time and insights. It has been very interesting speaking with you.

Robert Weiss | Of Counsel | Co-Chair, EV Initiative

Douglas Patton *is currently Principal of Jupiter Consulting LLC, an automotive consulting firm. Previously, he was CTO and EVP of Engineering at DENSO International America, Inc., and Senior Director of DENSO Corp. where he provided input and support on all aspects of R&D in North America.*

In his positions at DENSO, he oversaw all North American product engineering and development, campus facilities plus operations including all testing and technical services, and Engineering Administration. He was responsible for climate control, engine components, and systems and components, engine electrical, safety products, cluster, in-vehicle-infotainment (IVI), body electronics and small motor engineering.

Patton is currently Principal of Jupiter Consulting LLC where he provides support for Start-ups to Tier 1's in the rapidly changing automotive sectors of automation, electrification, security, and communication. This includes business strategy, technical direction, and industry requirement.

Patton is a member of the DENSO Foundation Board, the Transportation Improvement Board, the Engineering Advisory Council of Kettering University, and the advisory board of GAMIC start up competition.

In 2017 he served as president of the Society of Automotive Engineers. He was previously the president of the Engineering Society of Detroit. He is an Engineering Society of Detroit Fellow.

The Convergence of Electrification and AI
An Evolving and Uncharted Business and Legal Landscape

Tuesday, November 19, 2024, 3:30 – 7:30 | *MSU Executive Education Center, Troy, Michigan*

3:30 – 4 p.m.- Registration

4 p.m. Introduction and Overview

I. IntroductionModerator:

Bob Weiss: Welcome Remarks and Introduction of Speakers

II. Overview

Steve Wybo: Overview of the financial health of automotive suppliers and OEMs and how that health will affect EV and AI adoption.

4:30 p.m. First Panel

III. Intellectual Property Issues for AI and EVs

Joe Pytel: EVs and AI Fundamentals

IP Essentials related to AI and EVs; IP rights involving AI functionality; Copyright, Class Actions, Patent Preparation and Prosecution Issues; Software Patent Issues; Enforcement Strategies; Licensing and Transactions

IV. Cybersecurity

Greg Ewing and E.J. Hilbert: Cybersecurity Concerns Related to AI and EV Adoption are significant. Protecting Cars and Infrastructure, Regulatory Frameworks (including the U.S. and E.U.).

Break

5:30 p.m. - Second Panel

V. Legal Liability Issues Arising with Autonomous Driving Systems

Lael Andara: Overview/History of Autonomous Driving Systems and Liability; Federal and State Regulations; Class Actions; False Advertising; Product Liability; Case Studies; Safety and Public Perception; Insurance.

Who is responsible if an autonomous vehicle causes an accident -- The manufacturer, the software developer, the owner, or the passenger? What about unavoidable accidents?

VI. Privacy / AI Regulatory Framework

Greg Ewing: Privacy related to use of AI in EVs – EVs are essentially data collection machines: cameras, microphones, sensors, connected phones/apps. Data that could be problematic include facial expressions, sexual activity, seat-belt use, infotainment settings, destinations, and routes used, voice data and phone contacts, speed, among others.

Risks: Data sold to third parties, data breaches; expectation of privacy with EVs; fourth amendment questions; National Security Risks – in Feb. 2024, U.S. Dept. of Commerce opened investigation into risk of Chinese EVs; detailed information about U.S. infrastructure recorded; potential for cyber-attacks through control of vehicles.

Regulatory Frameworks: GDPR; US Regulations on Privacy–CCPA, etc.; future Federal Regulation; US Regulations on biometrics; AI Regulatory Frameworks; European AI Act

Q&A

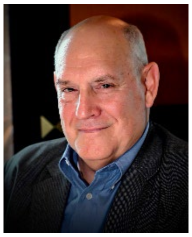
6:20-7:30 p.m. - Reception

CLICK HERE TO REGISTER

To learn more about our EV practice, visit our website at https://www.dickinson-wright.com/practice-areas/electric-vehicles?tab=0.

All views presented in this newsletter are those of the authors and do not necessarily reflect the views of Dickinson Wright.

Issue Authors:



Douglas Patton | *Principal* | *Jupiter Consulting LLC*
doug@jupiterconsultingllc.com

Gregory L. Ewing | *Member Partner*
GEwing@dickinsonwright.com
Tel.: 202-659-6954

Robert Weiss | *Of Counsel* | *Co-Chair, EV Initiative*
RWeiss@dickinsonwright.com
Tel.: 954-991-5455

Editor: ***Heather Frayre*** | *Member Partner* | *El Paso, TX*
HFrayre@dickinsonwright.com
Tel.: 915-541-9370