The 2020 Guide To Trends And Technology
For Smart Cities And Transportation

THE ROAD TO MOBILITY

BlackBerry

First Edition: The Road to Mobility
The 2020 Guide to Trends and Technology for Smart Cities and Transportation

Published by BlackBerry Limited, 2200 University Ave, E Waterloo, ON Canada N2K 047

To download PDF or e-book copies of the First Edition: The Road to Mobility visit:
http://blackberry.com/roadtomobility2020

Thanks to:
Edited By: Jeffrey Davis, Anthony Freed
Copy Editor: Carla Johnson
Project Manager: Swetha Sirupa
Executive Sponsor: Mark Wilson
Designer: Douglas Kraus

Read Blogs.BlackBerry.com, and follow us on Twitter (@BlackBerry) and LinkedIn (https://www.linkedin.com/company/blackberry/)

Table of Contents

Mobility Explodes Opportunities for Automotive. Let's Seize the Moment.

John Chen, *Executive Chairman and Chief Executive Officer*
BlackBerry

The future of transportation has captured people's imagination with its possibilities. Technology is enabling its transformation through expanded mobility options, smarter energy sources, and an underlying physical and technical infrastructure. Instead of thinking of cars as products to own, we're shifting mindsets toward transportation as a service with advancements like autonomous vehicles.

The global autonomous vehicle market accounted for US $27.9 billion in 2017. Forecasters expect a compounded annual growth rate of 41.5 percent through 2026, which would boost the market to US $615 billion. Add to that, autonomous vehicle adoption could reach 15 percent of global light vehicle sales by 2030.

While this progress toward modern mobility sounds positive, it comes with a multitude of complexities. A survey from the Ponemon Institute shows that 62 percent of auto manufacturers surveyed believe that they'll experience a malicious attack on their software or components within the next 12 months.

Another consideration that the Ponemon research brought to light is that 84 percent of automakers and their suppliers aren't sure that cybersecurity practices are keeping pace with evolving technologies. Thirty percent of survey respondents said they do not have an established product cybersecurity program or team. Further, 63 percent test less than half of their hardware, software and other technologies for vulnerabilities.

There's plenty that the automotive industry can control. But, do you know what steps you can take to avoid the potential damage cyberthreats can cause to your organization? To get started, I suggest you read this guide book, *The Road to Mobility: The 2020 Guide to Trends and Technology for Smart Cities and Transportation*.

The pages that follow provide a look into the future plus technical expertise from BlackBerry experts in automotive technology and security. We've also included insights from industry authorities and partners from ITSA, Metro21: Smart Cities

Institute at Carnegie Mellon University, Virgin Trains USA, the University of California, Davis, ISAC, Strategy Analytics, ISECOM, ICIT, CLTRea, Southwest Research Institute, and Cyber Future Foundation and Davos Cyber Future Dialogue.

After reading this guide, I invite you to visit the Automotive section of the *Inside BlackBerry Blog at* https://blogs.blackberry.com/en/category/industries/automotive for other helpful resources, follow us on Twitter @BlackBerry and LinkedIn to learn more about automotive security, and continue the conversation with one of the BlackBerry QNX or security experts on our team.

BlackBerry

The World of Smart Mobility

BlackBerry Smart Mobility Team

Our world is getting smarter and more connected day by day. Your smartphone controls your smart home. Your smart refrigerator orders groceries. Your smart doorbell lets you know when your guests arrive. Smart lighting helps you relax. And your smart thermostat makes sure you're comfortable while you move from room to room.

To a city, smart means better serving citizens, getting them to work in a safer, more reliable fashion, burning less fossil fuel, and building technology that fits their unique culture. For a technology company, it means an opportunity to refine data and use it for additional productivity. For an automaker, it means finding a new business model that fits with everchanging consumer habits.

Consumers see the advances in these other sectors and expect the automotive industry to follow suit – to take learnings from elsewhere and transplant them into experiences for their cars. This outlook has affected the shift toward mobility and optimism about what's possible. Emerging technologies are turning yesterday's science fiction into tomorrow's science fact. The speed of technology advancement has picked up at such a pace that many of these breakthroughs have delivered the future to our very doorstep.

Large companies are working hand-in-hand with cities and countries/states to find solutions to some of the biggest challenges we face: energy efficiency, climate change, congestion and equity. Start-ups are emerging every day addressing these same issues. Drones, cybersecurity, edge computing, cloud services and data science have made their way into the smart mobility world. This is where our focus as a company must rest — on the overall goals we are trying to achieve, and finding an understanding of each stakeholder's separate needs and where they intersect.

There's a strain as we look to find common ground between consumers, municipalities and businesses, how we each respond to contemporary situations, and how we ensure everyone's privacy and safety. The challenge remains in how we listen, talk and understand the vast needs and wants of all stakeholders.

With every new leap in technology comes uncertain ground. As consumers exert more influence and companies adjust to their expectations, emerging technologies produce unintended consequences. Public policies crafted in earlier eras are ill-equipped to govern today's dynamically-changing industry. This new world requires specific laws and regulations to govern the interactions between conventional cars, pedestrians and autonomous vehicles, as well as the data that can be derived from all of it.

The focus on laws and regulations should not be taken lightly. Cars are shifting from hardware machines to software platforms. As they become hyper-connected, they collect and analyze a great deal of information – not only about how you drive and where, but about the content that travels over a complex, interconnected network.

This information is key to increasing the safety of drivers, passengers and others on the road. It improves response time, helps avoid dangerous conditions and heightens the performance of the car. But, as more data is collected, consumers rightfully become concerned about privacy. What if my new software-defined car gets hacked?

It is this attention to safety and privacy that has amplified interest in security for the auto industry. We can't establish safety or privacy without a deep-dive into security. Many groups chose to push the security conversation to the background. At BlackBerry, we know that short-handed security solutions don't provide an acceptable level of privacy or safety. It has to be embedded at the outset, in the conception phase. Without this, it will be impossible for smart mobility to reach its full potential.

The auto industry is experiencing incredibly exciting times. The mindset, technology, regulation and partnerships that got us to where we are today will not be enough to sustain us going forward.

Instead of trying to push forward from the past, it's time to lead from the future.

Intelligent transportation is about more than getting from one place to another – it saves lives, connects worlds and creates opportunities. As a solution provider, BlackBerry is actively working to address the challenges and unintended consequences that come with these opportunities, so we can all safely and securely realize the benefits of smart mobility.

Charles Eagan is the Chief Technology Officer for BlackBerry. He oversees the advancement of new technologies, technology partnerships, and the standardization and integration of the company's products to support BlackBerry's Internet of Things platform.

SECTION 1

Creating a World of Safe, Secure and Smart Mobility

SECTION 1

Shifting from Conventional Transportation to Mobility on Demand

Shailen Bhatt, *President & CEO*
Intelligent Transportation Society of America (ITSA)

Sharon wakes up and already feels the weight of her day. When she bought her house in a new part of town five years ago, her 17-mile drive to work didn't take long. But now, the growing number of commuters who've done the same means she sits in traffic for more than an hour each way. The amount of unproductive time she spends weighs on her, as does the increased chances of a crash with more vehicles on the road. Sharon lives in an area filled with new builds, and the transportation infrastructure hasn't kept up with demand. Without other options, getting from home to work every day has added so much stress that she's weighing it against the cost of moving closer to her office.

According to U.S. Department of Transportation statistics, about 75 percent of U.S. workers like Sharon go back and forth to work in single-occupancy vehicles.[1] NPR reports that the number of commuters who spend 60-plus minutes traveling to work is on the upside of 14 million people.[2] Population growth in certain urban areas, like those where Sharon lives, and a booming job market mean that more people are traveling more miles each day. In addition to the billions of dollars and hours in unproductive time spent behind the wheel, this has also created an equivalent amount of wasted energy and greenhouse gases while increasing the likelihood of accidents and other issues.

While the majority of people in America have access to transit options, transit is facing some challenges. The transportation industry has built a system focused purely on moving cars. It's impossible to look at the infrastructure we've designed and expect to construct our way out of congestion. What we need to do instead of measuring vehicle volumes is focus on moving people, data and freight. This is where mobility comes in. People like Sharon are beginning to make choices that change their relationship with how they move from one place to another.

SECTION 1

The Need For Modern Mobility

The idea of mobility is a new concept, and it comes in many different forms. It could mean the people who used to spend the afternoon at the mall now have purchases delivered to their homes by drones. Instead of going out to eat, they use a meal service to deliver food for their dinner party. Instead of carpooling with neighbors down the block, they share rides with strangers going to the same destination. No more struggling to buy a first car to get to a job when you can choose where to work based on transportation options.

Mobility has become an important distinction because it means access. Access to work, healthcare, networks and family. Mobility delivers connections to the things we need in life. The greater our mobility, the greater our choices. Cultures and communities that lack flexible transportation options experience severe limits on life. Low-income people are trapped in a circle. They can't get to work because they don't have a way to get there. And they can't access commuting because they don't have a way to pay for it. The lives of older people aging out of driving changes dramatically once they don't have ready access to transit. A lack of mobility affects their physical and psychological health. And people with disabilities should be afforded the same access to mobility options.

Mobility on Demand (MOD) is transforming transportation today and will result in significantly different outcomes in the future. Mobility is driving the future of the relationships people have with their cars.

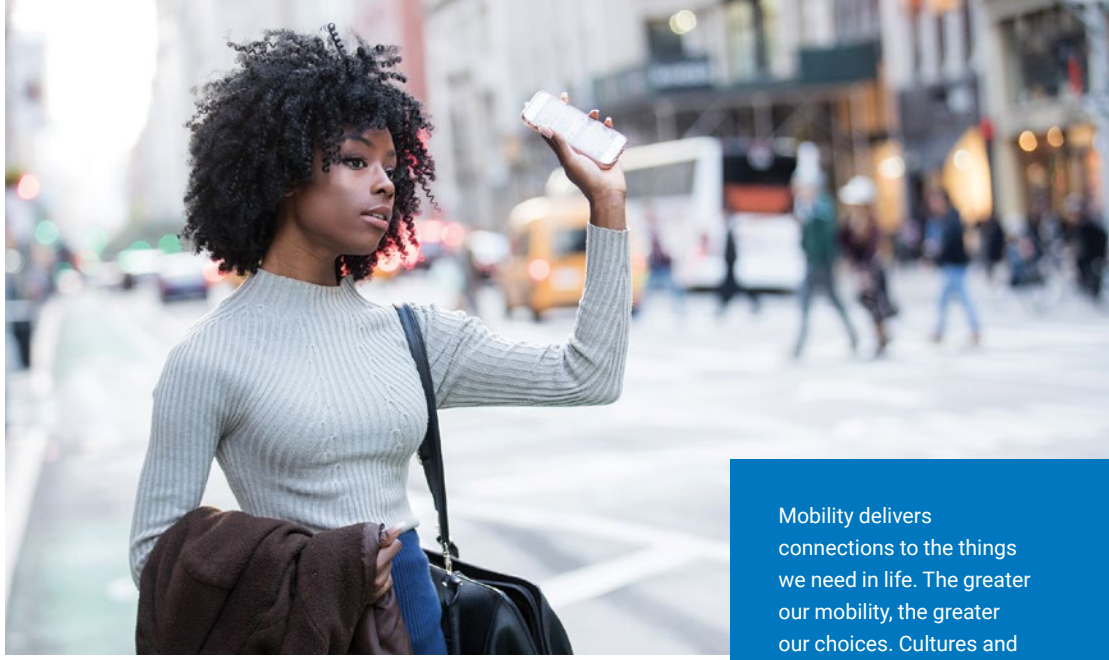
In the past, it was easy for people to own a car and drive anywhere. But today, because of big data and autonomous vehicles (AV), we can provide greater ride sharing or link multiple types of transportation together.

Whether it's new technology, such as AV, shared AV, ride sharing or new micro mobility options, people have more choices now because of the mobility revolution.

Convenient Connection Is Key

As we look at the issues that affect the maturity of transportation, one of the challenges is how to help people overcome the first- and last-mile piece of the puzzle. This is truly where MOD has come into play.

Previously, Sharon tried taking the bus to work, but it was a hit-and-miss experience. She left her home at the same time each day, yet sometimes she waited two minutes for the bus and others it was 20. The schedule was erratic and unpredictable, and she had precious time to spare in the morning. While the bus took her close to her office, she still had a substantial walk, which was hard to deal



Mobility delivers connections to the things we need in life. The greater our mobility, the greater our choices. Cultures and communities that lack flexible transportation options experience severe limits on life.

with in bad weather. At the end of a long day with darkness approaching, she looked for a taxi to take her to the bus. But because her office area had little demand after rush hour, a taxi was hard to find. That meant a long walk back to the bus and another jaunt at the end of the line to finally make it home. This experience was a poor option to sitting in gridlock during her commute.

Now, the city's bus schedule is updated in real-time and there is little guesswork. Sharon can choose the bus or a new light rail system that's been extended to her suburb. While it's further than a walk away, it's a quicker commute and she calls a ride-share service to take her there. Once she steps off near her office, a shared electric scooter service helps her cover the last bit of distance. On both ends of her commute, Sharon has reduced her stress and downtime while feeling good about safety and how her habits affect the environment.

Seamless Experience Through Single Payment

As MOD options increase, another hurdle is the cumbersome nature of paying for transportation. A bus takes one ticket and the train another. If people need MOD to get to their final destination, then it's a separate app or registration for a scooter, shared cycle or ride. If riders aren't prepared, it could cost precious minutes to reload a card and ensure there are no hiccups or missed connections along the journey. One city has done a brilliant job of tackling this challenge.

SECTION 1

In 2000, London created Transport for London (TfL), an integrated transport authority responsible for meeting requirements the mayor put in place. Specifically, these requirements state that by 2041, 80 percent of all journeys in the urban area will be made by foot, cycle or using public transport. As part of that initiative, TfL launched a contactless payment card called Oyster, which allows commuters to use a single card for payment and access to London's public transportation whether that be by bus, underground, over ground, rail, light rail, trams, roads, rivers, taxis, dial-a-ride or bicycles. This single adjustment to the city's fare system has saved millions of pounds a year.

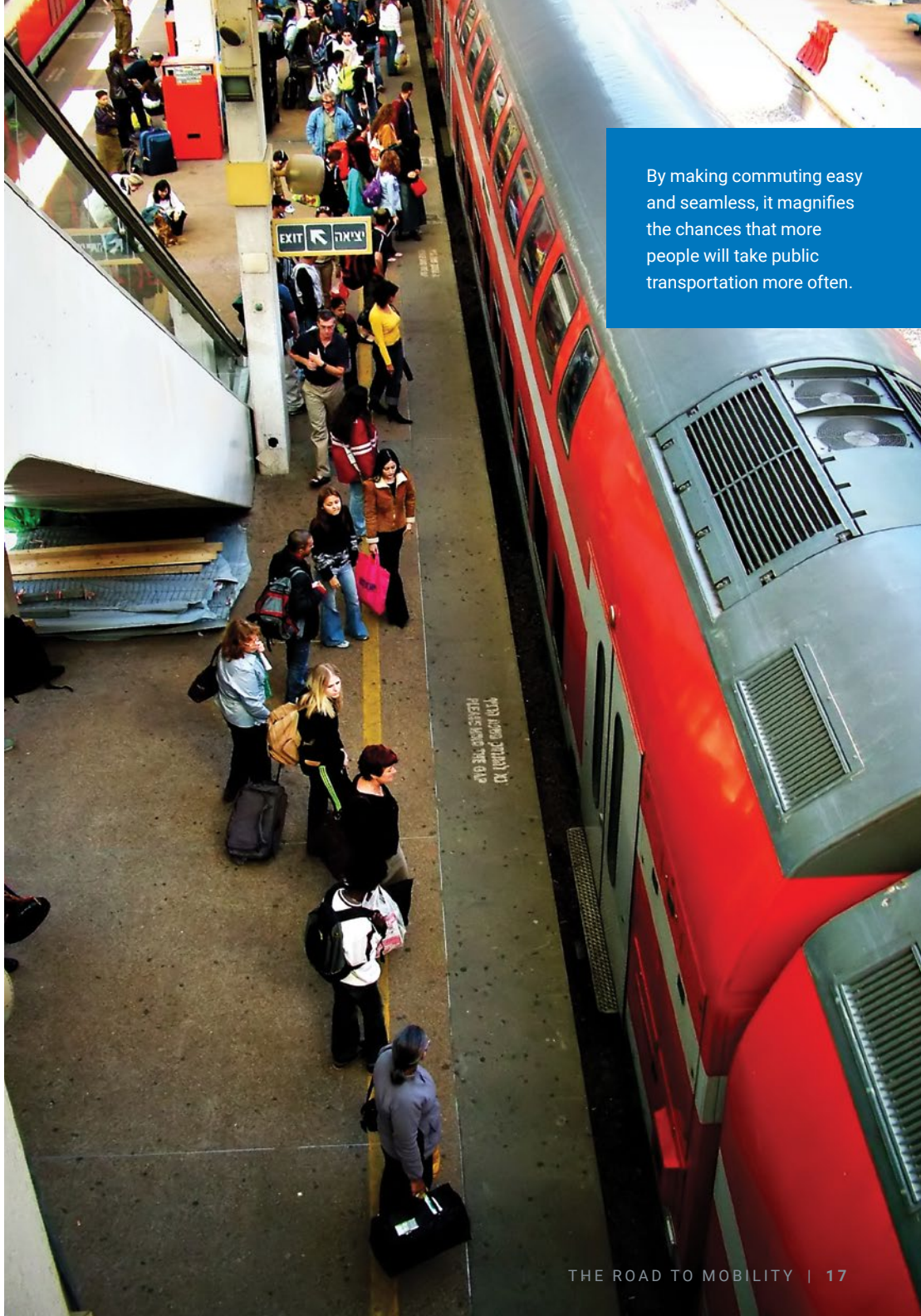
The results have been so successful that now urban centers in the United States are looking at how to implement a similar system. This includes Seattle with its One Regional Card for All (ORCA) system and New York City's Metropolitan Transportation Authority (MTA).

For densely populated urban areas, a single payment system can have a profound impact on MOD. By making commuting easy and seamless, it magnifies the chances that more people will take public transportation more often. It also points out that transportation authorities don't need to make massive changes to systems, they simply need to make systems more efficient. It's not realistic to expect everyone to use alternative options. However, if we can make it a better experience so more people will choose this option, we'll see the impact on congestion, environmental impact, downtime and expense.

Rethinking Mobility

MOD options and a seamless experience all come into play as we look at the changing dynamics of people's relationships with their cars. Research from the University of Michigan Transportation Research Institute shows that the percentage of people with a driver's license decreased across all age groups between 2011 and 2014. For people aged 16 to 44, the number has been decreasing steadily since 1983.[3] Earlier research showed two of the top three reasons for not getting a license include the cost of owning and maintaining a car and being able to access transportation in other ways.[4]

Car manufacturers are also taking note: people's views of cars are changing. No longer is the industry just about making cars, but rather becoming a transportation service provider. There will always be a certain segment of the population who drives their own cars. However, OEMs are looking to build relationships in order to deliver fleets of cars to other transportation providers. Daimler AG's car2go and BMW Group's DriveNow joined forces to create SHARE NOW. Through a single app, these companies can deliver five urban mobility needs in one solution — carsharing,



By making commuting easy and seamless, it magnifies the chances that more people will take public transportation more often.

SECTION 1

ride-hailing, multimodal trip-planning, parking and charging. The Maven platform offers a peer-to-peer car-sharing that lets GM owners list their cars and earn money. In Austin, Uber, Lyft, Postmates, GrubHub and InstaCart drivers who don't have their own vehicle can use Maven to rent an electric car for a price that includes insurance, maintenance and charging. This trend of transportation sharing will spread into the suburbs and more rural areas as car companies shift to selling mobility rather than just cars.

The other aspect of mobility is how people spend their time while in their cars. If people move to AV transportation, now the door is wide open about how people spend their time while en route. Pressed for time to prep for a work meeting? It's no problem in your AV because it's now your mobile office. You could hold video board meetings or connect with other offices so that wasted downtime turns into productive, revenue-generating sessions. If you need to commute between an airport and a final vacation destination, hospitality companies could start the experience earlier. Perhaps the AV delivers an environment that ties into the theme of the getaway — you step into a car that's now a tropical escape complete with views of an ever-stretching beach and stocked with tropical food and refreshments. Now, instead of the hassles of last-mile traffic, people arrive at their destination rested and relaxed.

What was previously an altruistic message to people like Sharon about driving less and riding more is now becoming a reality because of the growing MOD options and consumers' preference for them.

Fitting Puzzle Pieces Together

Transit is an important part of MOD because when it's done right, it can move a great deal of people efficiently. Urban centers are seeing people leave jobs because they can't afford basic transportation. Uber and Lyft have jumped in, but at the end of the day, we still have congestion. They give people the option to not buy a car, but by using them, riders still add to traffic congestion. Pools, however, are an option that makes transportation more efficient.

The popularity of bike sharing and scooters give evidence that the last mile connection is a missing niche in transportation. However, while the demand continues to increase for these options, discussions arise about where this traffic belongs — public streets may not be equipped to accommodate them, but pedestrians don't feel safe with their speed on the sidewalks.

While we have many decisions ahead of us and change seems cumbersome, we've made a great deal of progress in a short period of time. The technology revolution has given people alternatives to single-occupancy cars. What was previously an altruistic message to people like Sharon about driving less and riding more is now becoming a reality because of the growing MOD options and consumers' preference for them.

We're now able to look to the future and plan cities that look very different because of new transportation models. Smarter, more efficient mobility brings more benefits than just relieving congestion woes. Cities will create safer transportation systems that reduce fatalities, decrease greenhouse gas emissions and rid commuters like Sharon of stressful, unproductive hours.

Shailen P. Bhatt is President and CEO of the Intelligent Transportation Society of America (ITS America), where he promotes policies that advance the development and deployment of intelligent transportation technologies throughout the United States.

SECTION 1

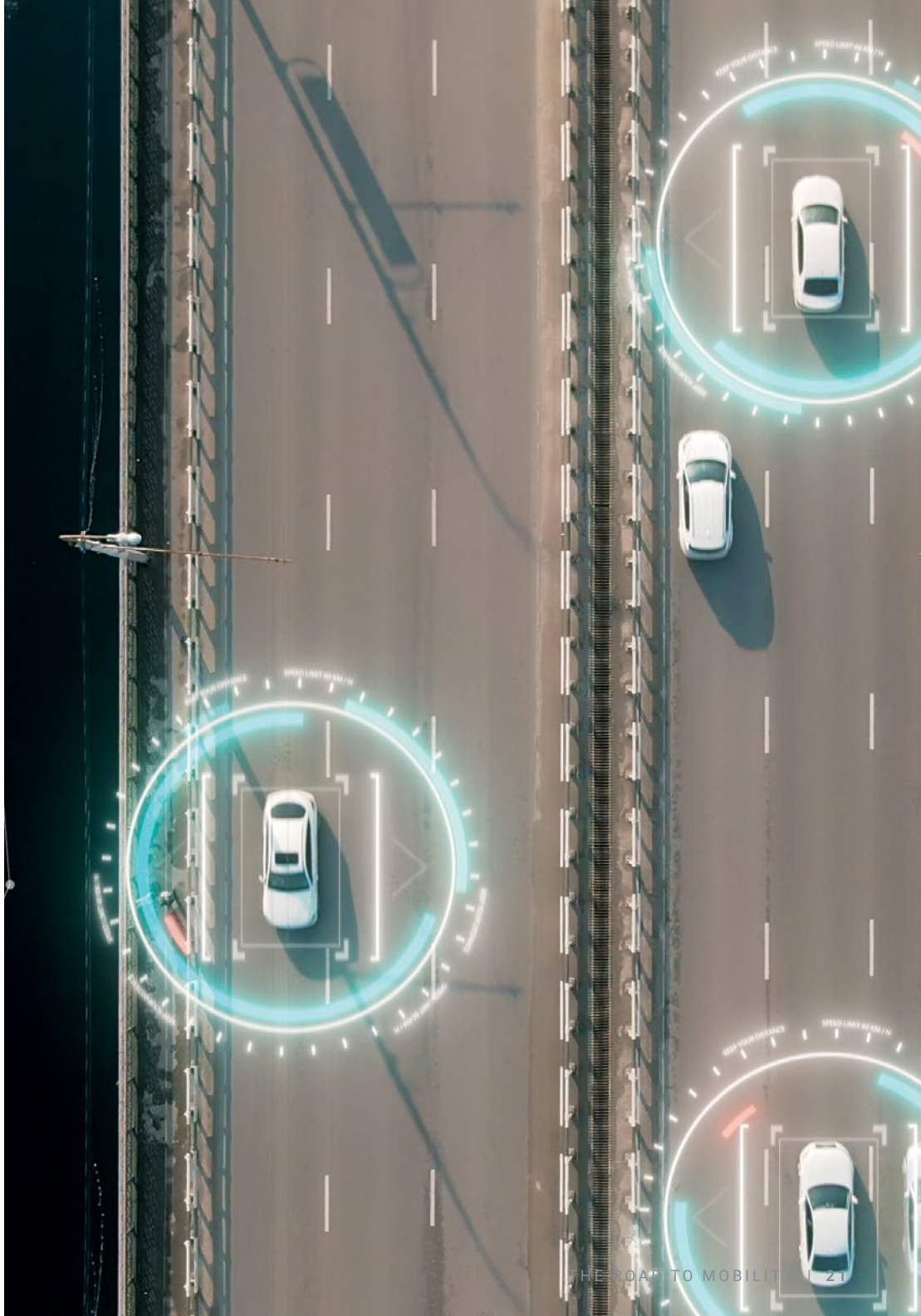
Safety as Standard: The Future of Smart Mobility

Karen Lightman, *Executive Director*
Metro21: Smart Cities Institute

When we talk about the development of smart city infrastructures, it is almost impossible to do so without prioritizing smart mobility. Mobility, or the ability to move or be moved freely and easily, is the backbone of any urban infrastructure. It powers a municipal economy by ensuring that employees are able to commute to and from their jobs in an efficient, frictionless manner. It ties neighborhoods together, enables children to attend school outside of their neighborhoods, bolsters the operation of hospitals and emergency response networks, and supports the maintenance of a robust infrastructure of roadways and public transit. As we move into the future of urban development and cities become more connected, focusing on mobility remains a key consideration in extending the benefits of smart city infrastructures to individuals at every economic and social level. However, overcoming the existing obstacles to smart mobility will require communication and cooperation between industry, regulatory bodies and the public, as well as a willingness to rethink existing urban paradigms to keep pace with the fast-changing transportation infrastructure.

The good news is that overcoming the barriers to introducing smart mobility solutions is ultimately not a technology problem. Innovations from vehicle connectivity to urban sensors have provided a strong technological foundation for smart infrastructures. That being said, putting one or one hundred sensors on a connected car will make very little difference without a clear platform or mission. Moreover, the integration of these technologies relies on ensuring that the necessary legislation and infrastructure are in place to support interoperability and to ensure data privacy and security, thereby building public trust. As such, the move to smart mobility solutions will not be as much an issue of research or development as an issue of deployment.

At Metro21: Smart Cities Institute[5] at Carnegie Mellon University, we have adopted a forward-looking creative approach to smart city development centered on RD&D (research, development and deployment). Throughout Metro21's work to bring



SECTION 1

people, technology and policy together to improve quality of life for metropolitan area residents, we have employed RD&D tactics that emphasize the importance of forging key partnerships between researchers, cities and government agencies to effectively incubate and incorporate the innovative technological systems driving smart cities of the future. Ultimately, technology is designed to serve a purpose and/or solve a problem. In this spirit, the future of smart mobility relies on a clear and equitable path to deploying these technologies.

Think of the airbag. Today, you'd be hard-pressed to find a car without one. However, when the airbag was first introduced commercially in the 1970s, this technology was not standardized or regulated. It took until 1998 — about 40 years after the first microelectromechanical automotive airbag system was patented — for federal legislation to mandate the installation of airbags in all new vehicles. In these intervening forty years, many automotive manufacturers had resisted the development and implementation of airbag requirements. As a result, the driver safety of vehicles varied significantly until airbag installation was standardized, effectively rendering safety a luxury for those who could afford it. As the transportation landscape is transformed through the development of new technology, notions of safety and equity can easily be treated as a luxury. This is where the government can collaborate with industry to promote equity in the deployment of new technologies.

Ultimately, technology is designed to serve a purpose and/or solve a problem, and in this spirit, the future of smart mobility relies on a clear and equitable path to deploying these technologies.

For instance, the City of Pittsburgh utilizes Surtrac, or Scalable Urban Traffic Control, in order to improve the accessibility of the city's roads to people with disabilities. Originally developed by researchers at Carnegie Mellon University's Robotics Institute, the Surtrac intelligent traffic signal control system adapts in real-time to shifts in urban traffic patterns. One aspect of this work involves the creation of a smartphone application that allows individuals who may need a bit more time crossing the road to increase the allotted time to go through a given intersection. By providing residents with disabilities with the ability to safely interact with their city's transportation infrastructure, municipalities can ensure that the benefits of smart mobility are not simply a luxury, but an improvement for all.

SECTION 1

Innovations in mobility will also prompt urban planners and policymakers alike to reimagine the way we utilize often-overlooked and under-regulated urban spaces to better support a more connected transportation infrastructure. For example, the advent of shared bike and scooter systems and ride-hailing services, such as Uber and Lyft, has significantly increased roadside congestion. Additionally, the increased utilization of goods drop-off services, such as Amazon Prime and Seamless, have also contributed to both urban congestion and emissions. While the curb has traditionally served as a meeting spot for buses, taxies and other high-occupancy transportation, as well as a space for parking cars, this new proliferation of low-occupancy vehicle traffic is prompting many cities to rethink how curb space could best support these new industries and maximize transportation efficiency without sacrificing sustainability. In collaboration with the City of Pittsburgh, Metro21 has developed a proof of concept[6] for a smart curb space. This framework would allow municipalities to optimize both automated and conventional methods of passenger drop-off and goods delivery, such as encouraging delivery trucks to make their drop-offs during off-peak hours.

To this end, as transportation becomes more autonomous, we must remember to enable sustainability at every step. As the integration of more and more autonomous transportation technology looms, municipalities will have to find innovative methods to mitigate the unintended environmental consequences of vehicle autonomy. Part of this will involve increasing the appeal of high-occupancy public transportation and shared mobility solutions. Currently, cities like Seattle and Los Angeles have expanded their use of bus-only lanes. As the name suggests, these lanes are specifically allocated for use by public buses. By shaping policy around the promotion of a transportation infrastructure (supplemented by technologies such as Surtrac) that prioritizes high-occupancy public transportation, such as buses and light rail, cities not only incentivize the use of these services by riders eager to reduce their commute, they also cut down on emissions generated by the new influx of low-occupancy vehicles and reduce traffic congestion. New technologies present promising opportunities to promote equity in transportation infrastructure. However, this will rely on cooperation between municipalities, government, industry and the public. Metro21 is well-positioned to be a neutral partner to help cultivate and grow those partnerships and we look forward to expanding the breadth and depth of our smart mobility and smart community deployment projects in collaboration with our growing list of partners.

Innovations in mobility will also prompt urban planners and policymakers alike to reimagine the way we utilize often-overlooked and under-regulated urban spaces to better support a more connected transportation infrastructure.

Karen Lightman is Executive Director of Metro21: Smart Cities Institute at Carnegie Mellon University. She's also an internationally recognized leader in building and supporting communities based on emerging technologies.

SECTION 1

The Now and the Near: How Futuristic Work Improves Transportation Today

Tina Quigley, *SVP Business Strategy*
Virgin Trains USA

Advanced mobility technology is disrupting the transportation industry and transforming how we will move people, goods and services in the future. Urban mobility, consumer expectations and technological capabilities are evolving at an extraordinary rate and disrupting how we traditionally deliver transportation services.

As we look at how to improve capacity and relieve congestion, it's time to realize we don't have room for any more surface level lanes. By thinking of "technology as the new asphalt," we can harness new technologies and integrate them into our existing infrastructure. We'll be able to deliver greater capacity and a higher return on investment compared to paving additional lane miles.

When it comes to the future of transportation, the Regional Transportation Commission of Southern Nevada (RTC) has pushed the boundaries on all that is possible by actively embracing technology. We've tested and implemented programs and practices in ways others haven't been able to. Because RTC holds responsibility for transit, roadway funding and traffic management, we're able to make decisions that have a comprehensive impact across all three areas.

We're on the threshold of transformative change in urban mobility. Emerging next-generation solutions are evolving rapidly and call into question the appropriateness of options the transportation industry has relied on for decades. While no one mode will solve all of our transportation issues, our goal at RTC is to build an interdependent, connected ecosystem of mobility that supports our residents and visitors. And, we plan to execute this in a way that ensures that our investments will be compatible with future technologies.

SECTION 1

For RTC, we have three strategic goals on which we focus to advance smart mobility in the Las Vegas Valley:

1. Connect People To Opportunities And Services

Consumer preferences and transportation choices are evolving. More and more residents and visitors are taking advantage of transportation network companies (TNCs) such as Lyft and Uber. For public transit to remain a viable option, the RTC is experimenting with technology and innovation to connect people more efficiently. We've had success with numerous programs that take unconventional approaches to keeping people connected.

Ride On-Demand Pilot Program

In 2018, the RTC launched a Ride On-Demand pilot program with Lyft and Tango Car. For the first time, we're able to offer paratransit customers a same-day transportation option. Nearly 250 paratransit clients have opted into the program and now have the ability to enjoy more flexible service.

Because of the unique needs of some of the passengers, Lyft educates its drivers on how to assist people with collapsible wheelchairs and supports low-vision and hard-of-hearing/deaf clients to ensure they receive the highest quality service. From February 2018 through August 2019, riders booked nearly 36,000 trips. In addition to cost savings, customers tell us that the service gives them a freedom they've never had before. This is the type of service the RTC hopes to continue to offer.

Since customers couldn't hail a wheelchair-accessible vehicle via Lyft in the same amount of time as a regular car, the RTC added another partner, Tango Car, to provide this service. While it costs more to subsidize this service, the addition meets the federally required parity mandate for paratransit customers. It also give us the option to make the program permanent in the future. Our partnership with both Lyft and Tango Car has delivered a 49 percent operating cost savings — more than $620,000. At the same time, wait times have gone down and service has improved.

Workforce Mobility Program

Created in partnership with Lyft, the Workforce Mobility Program (WMP) launched in October 2018. This initiative helps with the first- and last-mile transit gap in an area not served by the RTC system. This year-long pilot looks at how to meet the needs of people who work in the industrial area of Las Vegas — a growing part of the city, yet outside the regular transportation routes.

SECTION 1

Eighty employees of sports merchandise company Fanatics have registered for the Workforce Mobility Program. Lyft provides service to and from 13 specified RTC bus stops along six transit routes. The TNC provides the first- and last-mile service at a reduced rate, and the RTC subsidizes $1 per trip. Fanatics funds the balance for each employee trip. Between November 2018 and June 2019, workers have taken more than 900 Lyft rides, which often include more than one person per trip. These rides equate to 2,317 miles that employees would have had to walk to and from bus stops.

Had RTC extended just one transit route to service the area, the cost would have totaled $350,000 per year for service. Instead, as of June 2019 the total program price tag is less than $7,500. The Workforce Mobility Program is open to other area employers as well. At the end of this pilot, RTC staff will evaluate if and how to move forward with the program.

Aptiv

Las Vegas has over 45 million visitors each year and 2.2 million residents. People want on-demand transportation, which is evident in the 30-percent decline of riders on the transit system along the Las Vegas Strip. As the needs of travelers change, so do the services that RTC delivers. We view ourselves as a provider of mobility, not just a bus company, and we continue to investigate and offer options that help people move.

> **Passengers have described their rides as an amazing experience, been impressed with how technologically advanced the cars are, and felt safe and at ease.**

One of these initiatives is a partnership between RTC, Lyft and Aptiv. A global technology company, Aptiv develops "vehicle-to-everything" (V2E) technology needed for autonomous driving. This enables communication with locations, signs, traffic lights, other cars and pedestrians.

At the 2018 Consumer Electronics Show (CES), Aptiv conducted its largest, autonomous vehicle demonstration yet along the busy resort corridor with a longer route and more complex traffic scenarios. In partnership with Lyft, Aptiv's robot taxis provided more than 400 rides to approximately 20 pre-programmed destinations. Ninety-nine percent of the miles driven were done so autonomously. Even more impressive is that the trips earned an average rating of 4.997 stars out of a possible 5.

In May 2018, Aptiv and Lyft revived the project with 30 vehicles and offered the autonomous car option to riders traveling to and from 1,600 destinations across the Las Vegas Valley. In the largest commercial program of its kind in the United States, the Lyft and Aptiv partnership has provided more than 55,000 self-driving rides to more than 100,000 passengers with ratings on par with the CES demonstration. Passengers have described their rides as an amazing experience, been impressed with how technologically advanced the cars are, and felt safe and at ease. Ninety percent of passengers said they intend to hail another ride again.

These are a few of the examples of how RTC is reinventing what transit looks like, addressing the public's hesitation with autonomous vehicle technology and connecting more people efficiently without losing market share.

2. Increase Capacity, Improve Safety And Reduce Congestion

As traffic grows, RTC looks at ways to increase capacity yet address congestion. We can't pave more roads to keep pace with current growth, but smart transportation can help traffic flow more efficiently. With the number of visitors to Las Vegas, the city essentially hosts the equivalent of the Super Bowl every weekend, all year long. As we look at how to move millions of people throughout our region every day, two partnerships have proven to be particularly effective.

Waycare

One of our programs is a partnership between RTC's Traffic Management Center, Nevada Highway Patrol (NHP), the Nevada Department of Transportation (NDOT) and Waycare, one of the leading providers of AI-driven mobility solutions for smart cities. Waycare has been harnessing in-vehicle and city data, combined with predictive analytics, to provide traffic management and safety agencies with the ability to identify areas of roads at high risk for an incident and then activate preventative measures to those areas.

Waycare's crash prevention pilot program has reduced the number of primary crashes by 17 percent on one of the busiest stretches of Interstate 15 without requiring any additional resources from state or local agencies. During the program, 91 percent of drivers traveling over the speed limit reduced their velocity to below 65 MPH in the area where the team put speed reduction measures in place. The partnership has enabled the groups to identify and respond to crashes an average of 12 minutes faster, which means clearing incidents quicker, allowing traffic to flow sooner and reducing the chance of secondary accidents.

SECTION 1

Audi/Time to Green

Audi debuted a first-of-its-kind program called "Time to Green" in Southern Nevada in 2016. This traffic light information feature uses real-time information from connected traffic signals to provide motorists with a countdown to when a red light will turn green. This helps reduce stress and keep drivers more informed as they approach intersections. By the end of 2018, the feature was compatible with nearly 4,700 intersections nationwide.

In February 2019, Audi added a new feature to "Time to Green" called Green Light Optimization Speed Advisory (GLOSA). By advising drivers on the ideal speed to drive, this component helps them make green lights at intersections. This can help improve overall traffic flow and reduce fuel consumption by reducing the repeated acceleration and braking that happens at red lights.

This is a big step toward connecting vehicles with infrastructure. Eventually the information can be integrated into a vehicle's start/stop behavior, navigation system to optimize routing, and predictive services (such as suggesting an ideal speed to hit the most green lights in a sequence). All of these services are designed to either improve efficiency, drive time or traffic management.

3. Use Data Synergistically

The RTC's advanced tech initiatives yield massive amounts of data. There are inputs and outputs coming from a variety of systems: data from telematics on fleets; data within our traffic signals and cameras; and IoT devices like those found on orange cones. Data insights can yield solutions that help reduce congestion, improve mobility and enhance safety. For example, data can help improve traffic signal timing to create smoother commutes. All of this can tell a story whether it's independent or fused together with other sources.

> **Data insights can yield solutions that help reduce congestion, improve mobility and enhance safety.**

A priority for the RTC continues to be breaking down our own data silos and understanding the information we have. We're actively discovering data across all of our departments, which helps create a more comprehensive view of our traffic management operations. It helps us get a better look at the problems we're trying to solve, while proactively identifying potential problems and solutions. It also guides our understanding of how people move throughout the city. These insights show the challenges our residents and visitors face today while pointing out potential growth issues in the future. Knowing this, the RTC will be able to identify and implement programs that address the mobility needs of everyone.

Recently, the Commission convened a consortium of public and private Southern Nevada leaders across jurisdictions. The purpose is to establish a unified vision around what it means to be not just a smart city, but a smart community. And data is a driving pillar of that vision.

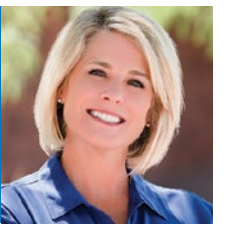
Through quarterly meetings and individual workgroups, we focus on establishing a framework for a regional platform to share and govern data. We work with public and private partners to collect GPS information from the roadway, including from public transit vehicles, other government entity fleets, traffic signals and mobile sources. This data is being used to better operate the traffic system and improve transportation operations throughout our valley.

While still in the early planning stages, we are working on a regional data management program that would allow all the data that is collected to be used by both the local jurisdictions and third-party providers.

The Future Of Transportation

No one mode will solve all of our transportation issues. But by building an integrated mobility system that delivers options for residents and visitors, the RTC has taken a big step forward. Southern Nevada is actively embracing technology while ensuring these decisions complement plans for future investments. Through numerous innovative projects and groundbreaking partnerships, we've become a leader in advancing smart mobility, because we realize how important it is to be forward-thinking and that we need to prepare for the future, today.

Tina Quigley is the SVP Business strategy at Virgin Trains USA. She is the former CEO for the Regional Transportation Commission of Southern Nevada, which oversees public transportation and metropolitan planning for more than 2.2 million residents and 45 million visitors annually.



SECTION 2

Emerging Technologies Shaping Mobility

SECTION 2

Security Confidence Through Artificial Intelligence and Machine Learning for Smart Mobility

Jeffrey Davis, *Head of Smart Transportation Innovation and Development*
BlackBerry
With the BlackBerry Cylance Data Science Team

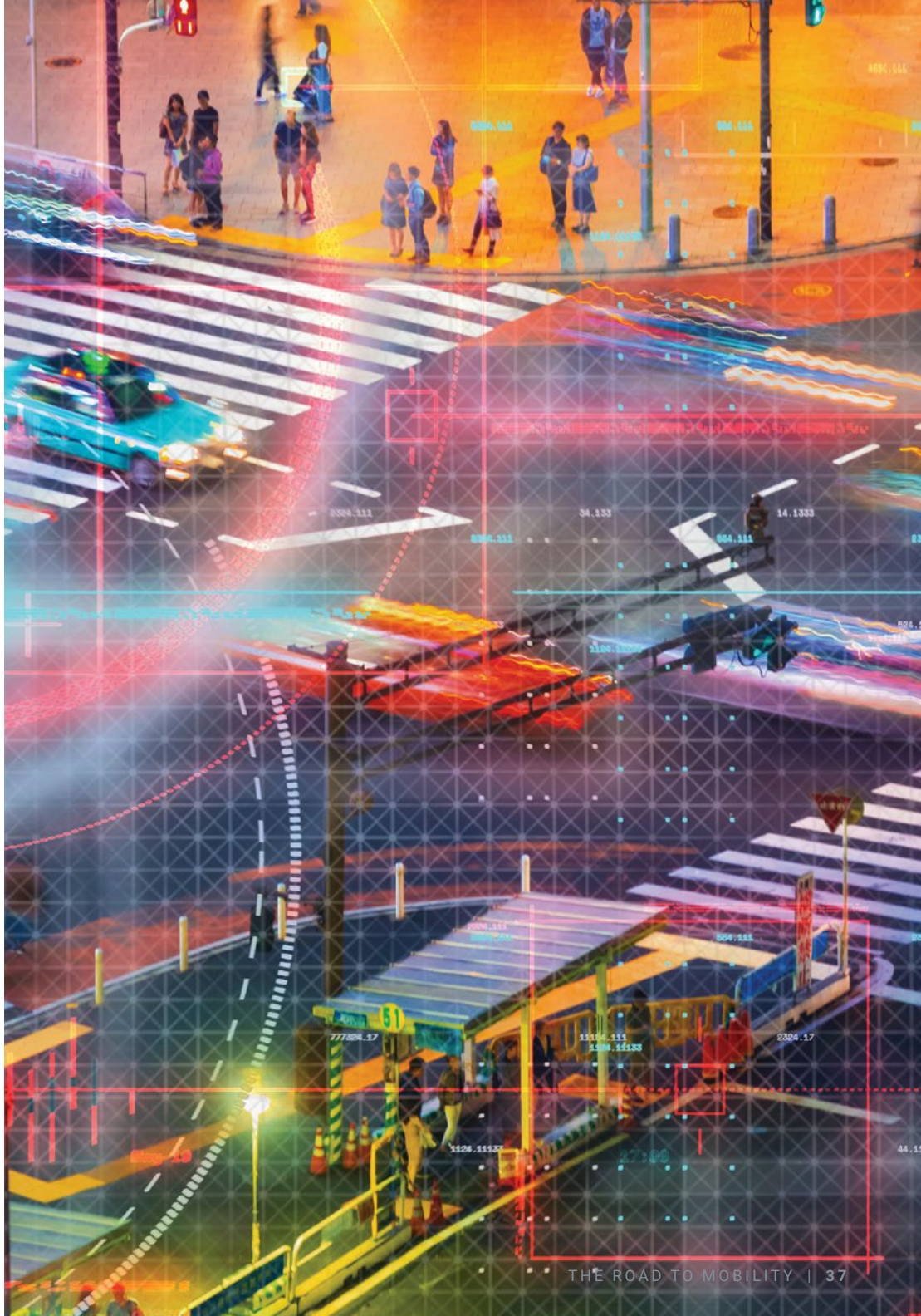
The world of mobility continues to grow and change. Automobiles, trains and traffic lights are moving from disparate parts of a loosely federated physical network to key nodes of operation on a far-reaching and virtually connected network. We are transitioning from industries driven from a central, top-down view to one focused on, and shaped by, the consumer.

In many ways, artificial intelligence (AI) and machine learning (ML) made this new focus a reality. From advancements in autonomous vehicles and signaling optimization to ride hailing and advanced mapping, all are made possible by forms of ML that, in some cases, operate through AI. In fact, every year machines do more and more to aid the world of transportation.

These machines pave a path to the goal of zero fatalities, zero emissions and zero congestion. They offer the hope of additional productivity and fair access to safe transportation. However, as we develop these complex technologies and combine them into complex systems, we need the help of machines to track and correct the actions of the network itself.

This is where AI and ML for enhancing security and safety outcomes offers us a chance to protect and improve our future. The ability to dynamically route vehicles, manage rules and ensure safe conduct can be done through supervised and unsupervised ML combined with planning, scheduling and optimization processing. Clustering, deep learning, planning and basic rule making addressing the challenge of identifying malware at endpoints, bad behavior within systems and correcting system errors.

AI provides the ability for humans to manage the chaos. People working at the intersection of technology and transportation have a requirement for a basic understanding of how AI works, common terminology and functionalities that are developing today. Cyber criminals, state-sponsored adversaries and competing



SECTION 2

organizations pose looming risks all through the mobility sector. Even more complicated is that the democratization of software across the application layer and throughout the Internet of Things (IOT) can create strain on a system that will most likely go unnoticed by human operators until there is an unwanted outcome.

It is imperative that professionals across the mobility sector have a basic understanding of what AI and ML really are beyond buzz words, what their capabilities and limitations are, how to know when to look for an AI/ML solution and what an appropriate solution looks like.

Technology advancements offer a chance to fix some very complex problems, but hype does not. The only way to fight hype is through knowledge, and this article is meant to be a starting point for your search. We hope you enjoy reading it as much as we enjoy sharing it, and we hope that it becomes a catalyst to drive more learning and curiosity about artificial intelligence.

Introduction To AI And ML Applications For Security

AI technologies are rapidly moving beyond the realms of academia and speculative fiction to enter the commercial mainstream. We now see innovative products using AI to transform how we access and leverage information.

AI is becoming strategically important to national defense. We also see it in securing critical financial, energy, intelligence and communications infrastructures against state-sponsored cyber-attacks.

> The era of AI has most definitely arrived. But, many still don't understand the basics of this important advancement, or how it could be applied to the cybersecurity industry.

According to an October 2016 report issued by the U.S. federal government's National Science and Technology Council Committee on Technology[7] (NSTCC), "AI has important applications in cybersecurity, and is expected to play an increasing role for both defensive and offensive cyber measures."[8] Based on this projection, the NSTCC has issued a *National Artificial Intelligence Research and Development Strategic Plan*[9] to guide federally-funded research and development.[10]

The era of AI has most definitely arrived. But, many people still don't understand the basics of this important advancement or how it could be applied to the cybersecurity industry.

AI: Perception Vs. Reality

The field of AI encompasses three distinct areas of research, on which we'll focus exclusively in this article:

1. **Artificial Superintelligence (ASI),** which is the kind popularized in speculative fiction and movies
2. **Artificial General Intelligence (AGI)** where machines are as intelligent as a human and equally capable of learning and reasoning
3. **Artificial Narrow Intelligence (ANI),** which exploits a computer's superior ability to process vast quantities of data and detect patterns and relationships.

In recent years, most of the fruitful research and advancements have come from ML, the sub-discipline of AI. ML focuses on teaching machines to learn by applying algorithms to data.

Machine Learning And The Security Domain

Context is critical in the security domain. Fortunately, the security domain generates huge quantities of data from logs, network sensors and endpoint agents, as well as from distributed directory and human resource systems that indicate which user activities are permissible and which are not.

Collectively, this mass of data can provide the contextual clues we need to identify and ameliorate threats, but only if we have tools capable of teasing them out. This is precisely the kind of processing in which ML excels.

By acquiring a broad understanding of the activity surrounding the assets under their control, ML systems make it possible for analysts to discern the relationship between events widely dispersed in time and across disparate hosts, users and networks. Properly applied, ML can provide the context we need to reduce the risks of a breach while significantly increasing the "cost of attack."

Clustering

The purpose of cluster analysis is to segregate data into a set of discrete groups or clusters based on similarities among their key features or attributes. Within a given cluster, data items will be more similar to one another than they are to data items within a different cluster.

In the network security domain, cluster analysis typically proceeds through a well-defined series of data preparation and analysis operations.

SECTION 2

We typically apply statistical sampling techniques that allow us to create a more manageable subset of the data for our analysis. The sample should reflect the characteristics of the total dataset as closely as possible, or the accuracy of results may be compromised.

Next, we decide which data elements within our samples to extract and subject to analysis. In ML, we refer to these data elements as "features," i.e., attributes or properties of the data that can be analyzed to produce useful insights.

In the security domain, the relevant features might include the percentage of ports that are open, closed or filtered, the application running on each of these ports and the application version numbers. If we're investigating the possibility of data exfiltration, we might want to include features for bandwidth utilization and login times.

Cluster Analysis

Cluster analysis introduces the concept of a "feature space" that can contain thousands of dimensions, one each for every feature in our sample set. At the conclusion of every clustering procedure, we're presented with a solution consisting of a set of clusters.

After completing this cluster analysis, we would expect to see the vast majority of the resulting data grouped into a set of well-defined clusters that reflect normal operational patterns, and a smaller number of very sparse clusters, or "noise points", that indicate anomalous user and network activity.

Cluster analysis introduces the concept of a "feature space" that can contain thousands of dimensions, one each for every feature in our sample set.

For security applications, we could then probe these anomalies further by grepping through our log data to match this suspect activity to possible bad actors.

Categorization

Categorization enables us to make generalizations about objects and actions we already know about in order to predict the properties of objects and actions that are entirely new to us.

In ML, classification refers to a set of computational methods for predicting the likelihood that a given sample belongs to a predefined class, like whether a piece of email belongs to the class "spam" or a network connection is benign or associated with a botnet. These examples illustrate a binary classification problem—for example, one with only two output classes, "spam" and "not spam," "botnet" or "benign."

The algorithms used to perform classification are referred to as "classifiers." There are numerous classifiers available to solve classification problems, each with its own strengths and weaknesses.

Supervised Vs. Unsupervised Learning

Classification is an example of *supervised learning*, in which an analyst builds a model with samples that have already been identified—or *labeled*—with respect to the property under investigation.

In contrast, clustering is an example of *unsupervised learning,* in which the properties that distinguish one group of samples from another must be discovered. It's not uncommon to use unsupervised and supervised methods in combination.

To produce an accurate model, analysts need to secure a sufficient quantity of data that has been correctly sampled and categorized. This data is then typically divided into two or three distinct sets for training, validation and testing. As a rule of thumb, the larger the training set, the more likely the classifier is to produce an accurate model.

A classification session typically proceeds through four phases:

1. A *training* or "learning" phase in which the analyst constructs a model by applying a classifier to a set of training data
2. A *validation* phase in which the analyst applies the validation data to the model in order to assess its accuracy
3. A *testing* phase to assess the model's accuracy with test data that was withheld from the training and validation processes
4. A *deployment* phase, in which the model is applied to predict the class membership of new, unlabeled data

In practice, an analyst may train and test multiple models using different algorithms and hyperparameter settings. Then, they can compare the models and choose the one that offers the optimal combination of accuracy.

SECTION 2

Classification Via Decision Trees

Decision tree (DT) algorithms determine whether a data point belongs to one class or another by defining a sequence of "if-then-else" decision rules that terminate in a class prediction. Decision trees are aptly named since they use roots, branches and leaves to produce class predictions.

During training, the resulting model will appear to provide a high degree of accuracy. When applied to test data, however, the accuracy scores will be much lower. Analysts refer to this as a *failure to generalize*.

The DT algorithm intrinsically generates a probability score for every class prediction in every leaf based on the proportion of positive and negative samples it contains. This is computed by dividing the number of samples of either class by the total number of samples in that leaf.

Once the DT model has been built, it's subjected to the same testing and validation procedures we described earlier for logistic regression. Once the model has been sufficiently validated, it can be deployed to classify new, unlabeled data.

Deep Learning And Neural Networks

Deep learning is based on a fundamentally different approach that incorporates layers of processing with each layer performing a different kind of calculation. Samples are processed layer-by-layer in stepwise fashion with the output of each layer providing the input for the next. At least one of these processing layers will be "hidden." It is this multi-layered approach, employing hidden layers, that distinguishes deep learning from all other machine learning methods.

> Like every important new technology, AI has occasioned both excitement and apprehension among industry experts and the popular media.

The term *deep learning* encompasses a wide range of unsupervised, semi-supervised, supervised and reinforcement learning methods primarily based on the use of neural networks, a class of algorithms so named because they simulate the ways densely interconnected networks of neurons interact in the brain.

Neural networks are extremely flexible, general-purpose algorithms that can solve a myriad of problems in a myriad of ways. Unlike other algorithms, for example, neural networks can have millions, or even billions of parameters applied to define a model.

After each training cycle, a loss function compares the classification decision assigned at the output layer to the class labels in the training set. This determines how to modify the weights in all of the hidden layers to produce a more accurate result.

This process repeats as many times as required before a set of candidate models can proceed to the validation and testing phases.

Conclusion

Like every important new technology, AI has occasioned both excitement and apprehension among industry experts and the popular media. We read about computers that beat Chess and Go masters, about the imminent superiority of self-driving cars, and about concerns by some ethicists that machines could one day take over and make humans obsolete.

We believe that some of these fears are over-stated. We also stand behind the idea that AI will play a positive role in our lives as long as AI research and development is guided by sound ethical principles that ensure the systems we build are fully transparent and accountable to humans.

In the near-term, however, we think it's important for security professionals to gain a practical understanding about what AI is, what it can do, and why it's becoming increasingly important to our careers and the ways we approach real-world security problems.

As Senior Director, Connected Transportation for BlackBerry, Jeffery Davis holds responsibility for the strategic innovation and development of smart transportation markets. He's developed cybersecurity, mobility and connectivity programs that specifically focus on human interaction with advanced technologies and new concepts.

SECTION 2

Intelligent Transportation Systems: Hurdles, Hopes and Highpoints

Jim Alfred, *Vice President*
BlackBerry Certicom

The move towards Intelligent Transportation Systems (ITS) is becoming a global phenomenon. New computing, sensor and communications technology pave the way for smart roadways, and cooperative and autonomous driving technologies. Forward-looking governments harness this technology to shape the future, providing economic, environmental and social benefits for their citizens.

The Benefits Of ITS

ITS has the potential to deliver numerous benefits to the transportation industry, the environment, consumers and governments. Specifically:

- ITS drives large-scale economic benefits through transportation efficiency
  - Sharing real-time vehicle and infrastructure data reduces traffic congestion and delays
    - This increases business productivity and enables just-in-time manufacturing
    - Saving fuel means a lower demand for imported fuel, which helps reduce trade deficits
    - Commuters will experience improvements, which increases employee productivity with the potential for better work/life balance
- Data provides visibility that can help optimize infrastructure spending
  - Lower operational and maintenance cost for infrastructure can reduce long-term tax burdens
- Data provides trends to help shape transportation and urban planning policies
  - By identifying where to expand and where to shed excess capacity, which helps areas such as urban planning
  - This helps prioritize spending, for instance which roads or bridges need repair now and which can wait

- There's now a way to enable safe increases in speed limits that can boost traffic capacity with little cost

- ITS helps protect the environment from climate change
  - Reduced traffic congestion can dramatically reduce greenhouse gas emissions
    - A study in Japan suggest ITS can reduce CO2 emissions by 40 percent for cities with high-traffic congestion
    - Security mechanisms can help local governments enforce road management policies

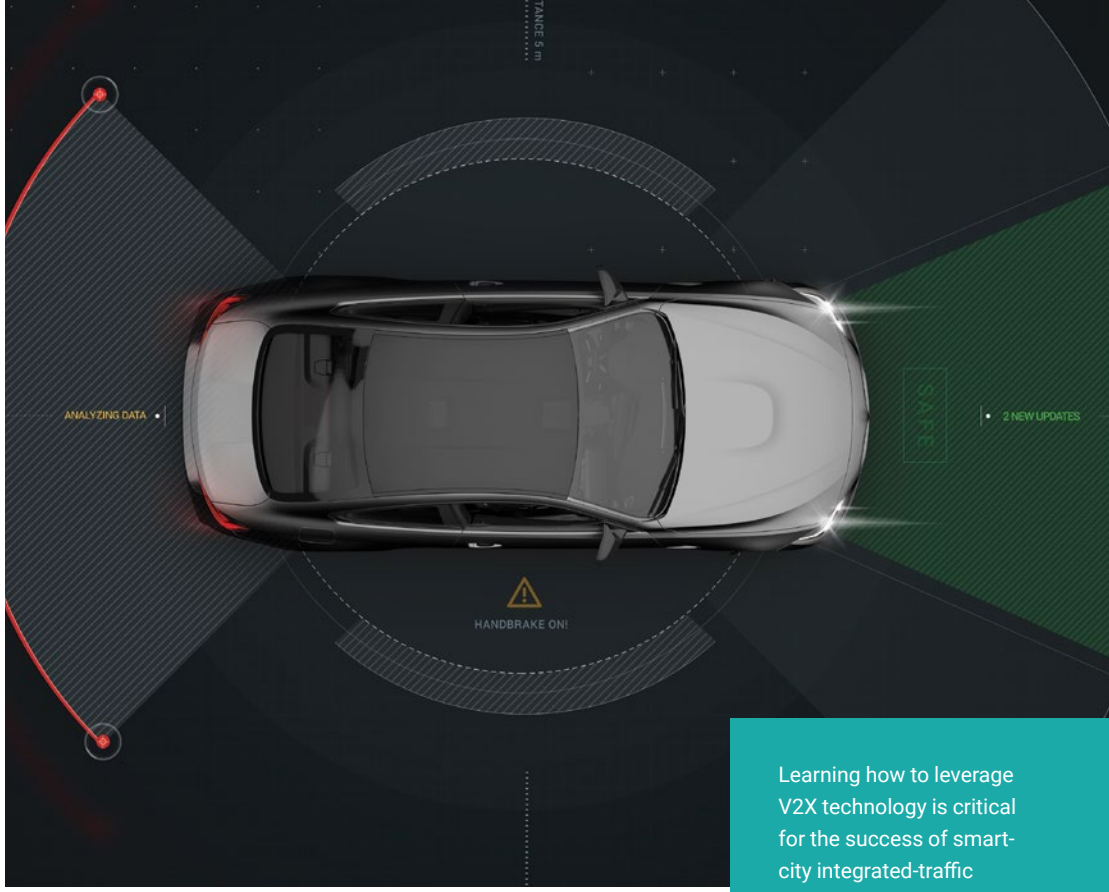
- ITS can improve road safety and saves lives with new collision-avoidance technology
  - Analysis published in the January 2017 Federal Register (Vol. 82)[11] indicates that over the next 30 years new collision avoidance technology might prevent some 500,000 U.S. vehicle crashes

The Challenges

The automotive industry and its ecosystem of silicon and software suppliers has made great progress in developing and proving out the technical aspects of ITS through long-term government-supported investment. One of the key enabling technologies for ITS comes from the communications between cars and the roadside infrastructure. Vehicle-to-everything, or V2X communications, helps enable vehicles to drive cooperatively, avoid collisions, and share data with city traffic management systems about traffic and road conditions. Core concepts of V2X technology developed in the early 2000s have come into their own through extensive piloting in the past several years. The barriers to adoption are now largely policy and economics-based rather than technical.

Different regions (North America, Europe and Asia) will naturally see policy challenges with a unique perspective. For instance, the European Union (EU) has long grappled with the aspect of supporting a wide variety of member states and industry stakeholders while giving each a voice.

For international standards, too many stakeholders can pose a real problem. But to its credit, the EU, working through the Car2Car Consortium and ETSI, has developed a strong, viable standard. To enforce technical and security compliance, EU V2X stakeholders have developed a centralized governance model and technical interlocks for managing duly qualified participants in the European V2X marketplace. The EU's C-ITS Credential Management System (CCMS) has first established out a



Learning how to leverage V2X technology is critical for the success of smart-city integrated-traffic management initiatives. These benefits could help fund V2X deployments and smart city evolution.

central policy for how trusted elements of the system operate. Once operational, it will then allow governments, OEMs and service providers an opportunity to deploy any systems that meet its security and interoperability requirements. By bridging trust at the policy level, the European Union has eliminated a major barrier for ITS adoption in Europe.

Kudos to the European V2X community for a job well done. Coordinated action by member states and industry stakeholders will help pull the benefits of ITS forward. This will address growing concerns about the acceleration of climate change, over-reliance on fossil fuels and a strong growth in road traffic densities.

China, likewise, has embraced the benefits of ITS to transform its roads and highways. They are working to accomplish their objectives by tying V2X to a vision for smart cities enabled by 5G cellular services. Their goal is to leapfrog western technologies and bring cellular V2X (C-V2X) based on 5G technology

to life. Chinese standards organizations, industry stakeholders and government authorities are driving fast and certain deployment goals. There seems to be little concern about interoperability with Western V2X PKI systems, which is easy to understand. China is an enormous market and a national ITS standard delivers a route to domestic ITS technology dominance.

The United States, which has arguably invested the most in C-ITS, may have the least to show for it. While DSRC-based V2X technology stands potentially at the ready, lack of a coherent government policy and robust coordination between North American governments has led the industry to an uncertain stall. Without a V2X mandate or other incentive, automotive OEMs lack reasons to invest on their own. Unless North America develops stronger leadership, it may see the V2X-enabled ITS opportunity pass by as other industries lobby the FCC for access to the U.S. ITS safety spectrum.

To overcome the challenges, U.S. and Canadian government and automotive industry leaders must work together to develop a regulatory framework that promotes the benefits of ITS and V2X technology. They must also explore industry incentives that helps the market align benefits to cost.

Lacking a U.S. mandate, why should OEMs spend money to put V2X modules in every car? Because the safety benefits will not accrue to them in higher vehicle prices or sales margins. Perversely, fewer accidents would mean fewer new car sales, which is not much of an OEM incentive. And were OEMs not properly incentivized, a likely scenario is that V2X would be seen as an expensive safety option that few consumers would purchase, leading to a lower installed base and a less-effective system.

Coordinated regulation could easily turn this around. For instance, if we assume V2X adoption will improve traffic flows and reduce congestion, then it seems reasonable that vehicles with V2X technology would achieve better fuel economy. Perhaps that's a good reason to give each vehicle manufactured with a V2X module a credit on the manufacture's CAFE standard and thus an incentive to sell cars with V2X modules as standard equipment.

And, let's assume consumers benefit from better fuel efficiency as well as safer roads. Safer roads should lower vehicle owner insurance premiums. This provides justification to require car owners to pay for safety certificates to prove their cars and V2X modules are in good working order. That money could in turn be used to help fund state and local ITS deployments.

Finally, let's not ignore the ability of V2X modules to support value-added services. For example, they offer a way for cities to monetize services such as freight signal priority for trucks or license access to special V2X-vehicle-equipped commuter lanes. Learning how to leverage V2X technology is critical for the success of smart-city integrated-traffic management initiatives. These benefits could help fund V2X deployments and smart city evolution.

Together, supportive policies and practical applications can help catalyze the North American ITS industry.

BlackBerry's Security Credential Management System (SCMS)

The SCMS, a large-scale distributed public key infrastructure (PKI) used to secure V2X communications, is an integral part of the V2X system. This enables trust in messages from vehicles, traffic management and other infrastructures. Wireless messaging between cars and infrastructure is secured using digital signatures based on Elliptic Curve Cryptography (ECC). The trust model is based on a certificate scheme invented by BlackBerry Certicom and pledged with patent assurances to the broader community.

BlackBerry has built its system to North American specifications and proven multi-root interoperability through industry testing. We recently launched our WebTrust-audited SCMS service and are offering free V2X connected vehicle pilots. Unlike Europe, there are no formal governance rules dictating how to operate such a system in the U.S. or Canada. Lacking a government or industry sanctioned governance framework, we have adopted our own stringent PKI policies, adopting many of the practices dictated by the EU's V2X credential management policy framework. We would not simply say "trust us, we're BlackBerry," but rather encourage the automotive industry to work with us to create a secure, interoperable and sustainable intelligent transportation system.

Jim Alfred serves as the Certicom General Manager and Vice President of BlackBerry Technology Solutions. In his work, he provides specialized security solutions to the embedded, mobile and IoT market.

SECTION 2

The Signal and the Noise: The Car of the Future as a Software Platform

John Wall, *Senior Vice President*
BlackBerry Technology Solutions

The topics of self-driving cars and electric vehicles have sparked a frenzy of conversations. Consumers and manufacturers are fascinated by the potential these changes are bound to bring. All eyes are on the impact on society, the environment and the entire transportation industry. Autonomous cars will maneuver the rush-hour traffic and park themselves. There's opportunity for fractional car ownership and dialogue around ownerless transportation. Consumers ask, "how close are we to a self-driving world?"

These discussions, however, are mere noise compared to the underlying signal of where the automotive industry is really headed. The bigger conversation that's brewing is the software that's driving the transition to the next generation of automotive architecture.

Getting Our Bearings

The forecast for autonomous vehicles says that growth will crescendo over the next 15 to 20 years as the industry moves toward level 4 and 5 technologies. We're already well on our way. In May 2019, Lyft's self-driving car service in Las Vegas surpassed 50,000 riders[12]. Uber's self-driving car unit is attracting billions in investment.[13] Google's prodigy Waymo claims that it's building the world's most experienced drivers. The speed, however, will be impacted by the regulatory environment, cybersecurity and, in particular, software.

The world has more than 1.25 billion passenger cars, but less than 6 percent are connected to the cloud. By 2020, that number will soar to 20 percent. Public and private collaboration, innovation, such as the 5G network, and increased investment are fueling this trend. The benefits are considerable, including increased safety, reduced traffic congestion and emissions, greater highway capacity and productivity, improved mobility, smarter cities and rapid innovation.

SECTION 2

As we look at today's cars, they house 60-100 or more Electric Control Units (ECUs) across six to eight operating systems. Today's luxury vehicles contain upward of 130 ECUs with more than a million lines of code, making them more intricate systems than a Boeing 787 Dreamliner or Lockheed Martin's F-35 Lightening II fighter. These isolated operations increase the cost and weight of the vehicle, add complexity, increase the security risks by attack vendors and surfaces, and ultimately, offer little opportunity to upgrade the system.

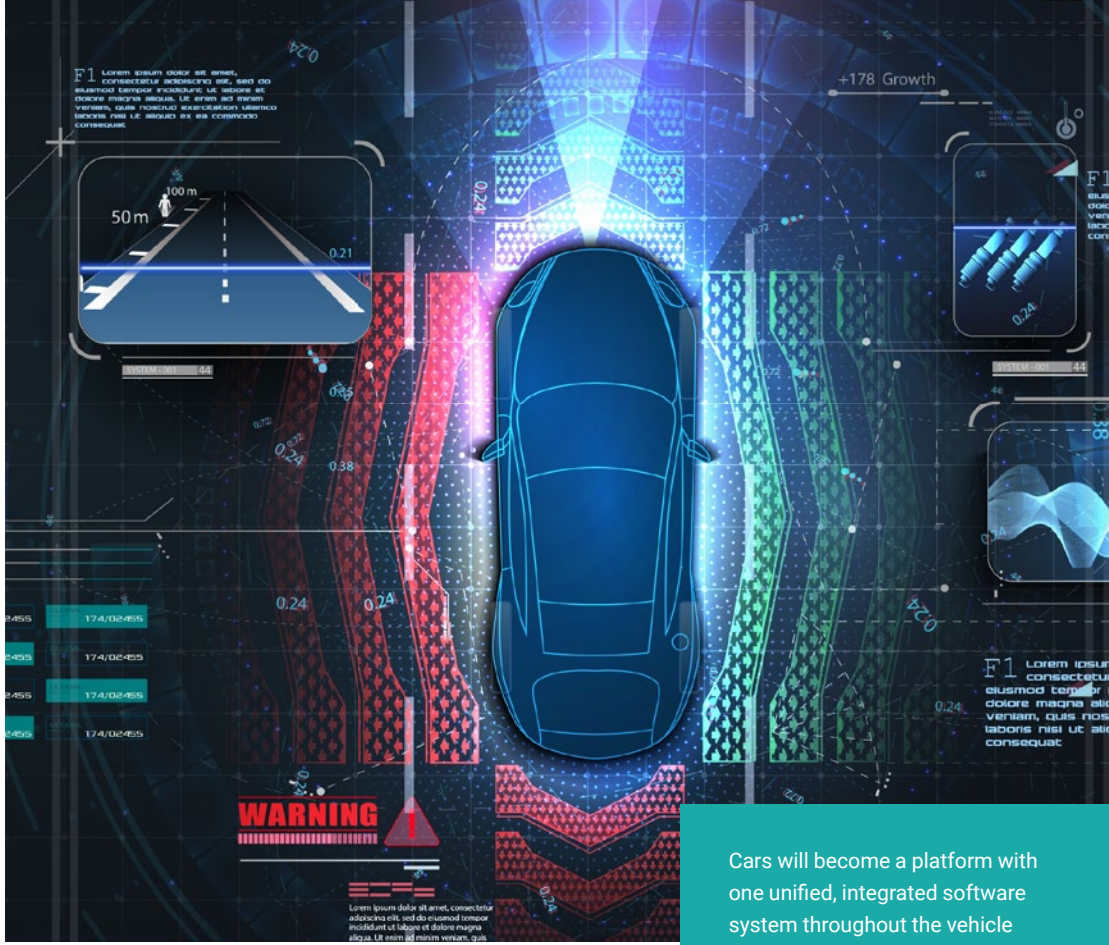
However, tomorrow's software opportunity means we'll see small ECUs collapse into six to 10 High-Performance Computer (HPC) platforms. These coordinated software systems will house coordinated operations that reduce the weight, cost and complexity of vehicles. They'll also future-proof cars with the power to upgrade already built-in.

The ECU consolidation offers bountiful benefits. The entire process will be simpler for designers, engineers, procurement, production and inventory management. Consolidating the controls mean less wiring, which means less weight. That, in turn, improves the fuel economy and cost of the car.

The Connected Car

As the demand for autonomous cars gains speed, the software opportunity will grow along with it. Experts estimate that today's $0.5 billion software market will jump to $10 billion in 2020 and a booming $25 billion in 2030. It's estimated that by 2030, 50 percent of a cars' build of material will be electronics and of that, 30 percent will be software. This creates a tremendous opportunity for OEMs wanting to create serious differentiation in an environment that's constrained by complexity, liability and low margins.

In the future, the industry will have a common hardware leading to more cohesive software. Cars will become a platform with one unified, integrated software system throughout the vehicle allowing all parts to connect and communicate with each other. OEMs are taking notice and increasing software and IT investments. In 2017, Ford hired 400 BlackBerry engineers to drive their connect car development focus. Toyota invested $1 billion in Silicon Valley with the goal of playing shoulder-to-shoulder with Google and Apple. GM Canada hired 700 engineers to drive research in self-driving cars. GM also increased the number of its tech workers by eight-fold between 2012 and 2017. These OEMs understand that to increase profits, providing services through the car will be key.



Cars will become a platform with one unified, integrated software system throughout the vehicle allowing all parts to connect and communicate with each other.

What's happening in the industry, while complex, resembles the mobile to smart phone migration. Look back 10 to 15 years and the communications industry had numerous players providing mobile devices with diverse ecosystems and no common software platform. People now manage nearly every aspect of their lives from the palm of their hand. Apps transformed mobile phones into highly productive work and entertainment devices. Smartphones quickly evolved from devices for saving appointments and delivering a few basic corporate applications into handheld computers capable of making phone calls.

If we think about the car of the future, we can draw parallels between what's coming and what's happened with smart phones. The mobile industry found itself at the intersection of several others — communications, computing, media, consumer

SECTION 2

electronics and mobile commerce. The smart phone brought convergence and gave people a good ecosystem, a simple user interface and software — in the form of apps — that changed the landscape of the industry and put the internet at people's fingertips.

We'll see autonomous driving, safety components and other features as a choice for a downloadable app rather than a dealer option. Google entered the autonomous vehicle market with subsidiary Waymo's taxiapp already available in the Play Store. The Tesla app puts owners in direct communication with their vehicles and Powerwalls anytime, anywhere. We'll see app after app pop up. However, just like the early days of the smartphone, each one is built on a different platform with different software requirements.

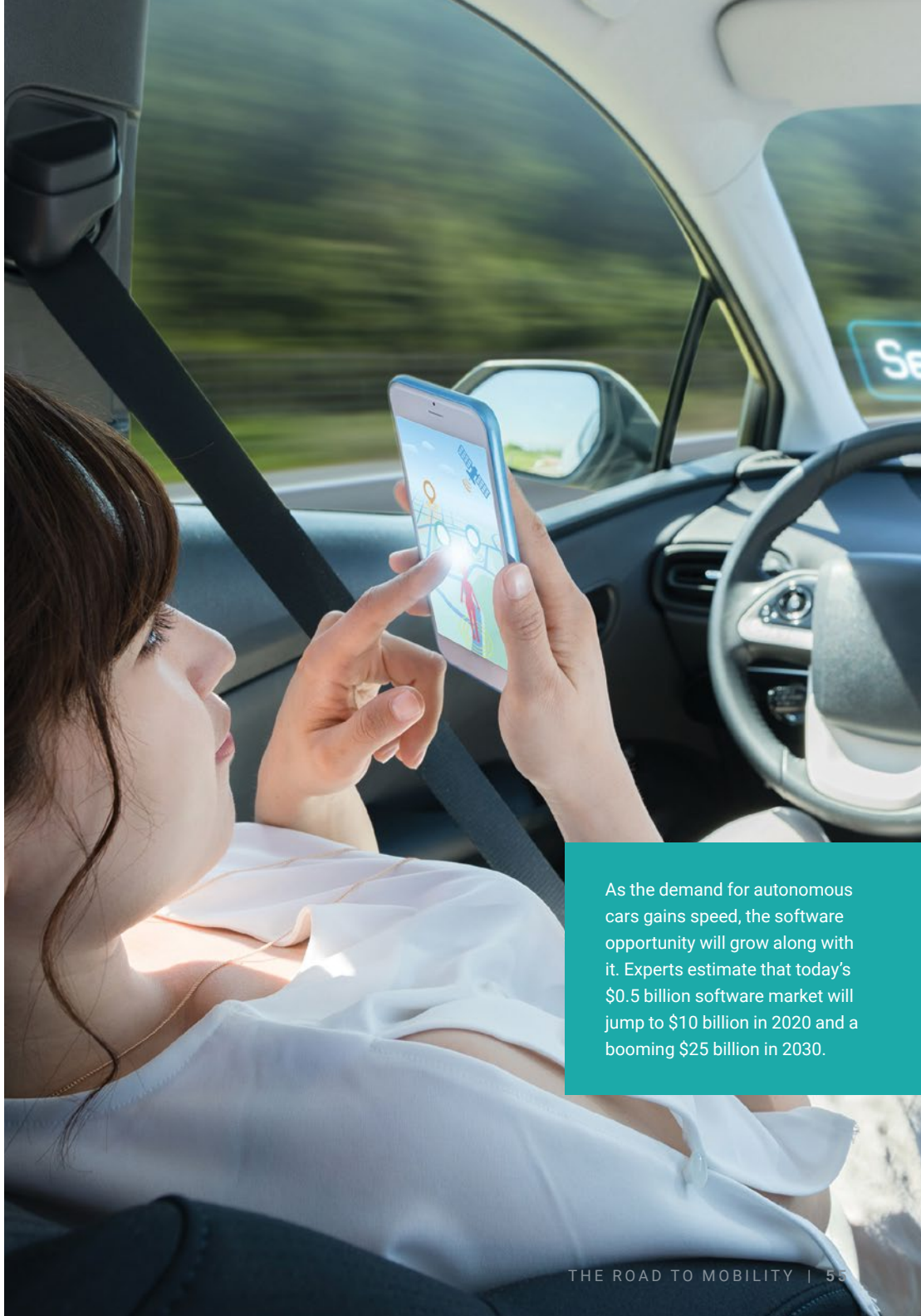
Technology convergence is pushing alliances between once isolated business industries, which is why we see the new partnerships being developed between General Motors and Lyft, Fiat-Chrysler and Google, and Samsung and Harman. Convergence is taking place between automotive, technology and telecom to serve consumer demand for automated driving, connectivity and shared mobility.

The Software Opportunity

In the future, the software ecosystem in the automotive industry will converge the same way it did with smartphones. And just like the mobile industry has evolved from numerous operating systems and narrowed down to iOS® and Android™, the road will narrow in the same way with a common software platform for automobiles. The companies who will thrive in this transition are those who understand the software architecture of the car, whether that's OEMs from the hardware point of view or software savants like Google.

> **Convergence is taking place between automotive, technology and telecom to serve consumer demand for automated driving, connectivity and shared mobility.**

The difference between phones and cars is that the standards for the mobile industry don't meet the strict safety and security requirements of automobiles. Even though cars will become a service that function through apps, current iOS and Android-level environments lack the mission-critical criteria for control. The four areas of concern include:



As the demand for autonomous cars gains speed, the software opportunity will grow along with it. Experts estimate that today's $0.5 billion software market will jump to $10 billion in 2020 and a booming $25 billion in 2030.

SECTION 2

1 **Real-time.** iOS and Android aren't true real-time operating systems because of their bounded latency. Converged networks that support an app ecosystem in the auto industry must be deterministic.

2 **Robust.** Today, roughly 6 percent of cars are connected to the cloud but the industry estimates that number will grow by 250 million 2020. This pace will increase even faster with the introduction of the 5G network in the near future.

3 **Security.** The threats against connected cars are increasing. The primary properties that will be critical to the car will be a high-level of security along with functional safety performance that meets 61508 — ISO 26262 standards. When connecting to the cloud, there can be no safety without security.

4 **Safety certified.** As vehicles get more sensors for assisted driving, they'll collect more data about the environment, which they will then have the opportunity to monetize. This offers golden egg for every OEM.

Monetizing The data

The automotive industry is rife with complexity, liability and pressure to grow margins. There's a chance to shift the economics by focusing on software, however, which is clear based on the interest that's spiking from companies like Apple and Google. The opportunity lies in the data that's collected from the software.

Intel[14] estimates that every autonomous car will generate the data equivalent of almost 3,000 people. Dig deeper and multiply that by the number of people on the road. Assume even 1 million autonomous cars worldwide and that means automated driving will represent the data of 3 billion people.

> **McKinsey's 2016 study *Monetizing Car Data* reports that the overall revenue pool from car data monetization at a global scale may total as much as $450-750 billion by 2030.**

McKinsey's 2016 study *Monetizing Car Data*[15] reports that the overall revenue pool from car data monetization at a global scale may total as much as $450-750 billion by 2030. Auto execs say one connected car generates 10 times more revenue than a conventional vehicle. OEMs understand that future revenue streams hinge on their ability to develop new business models including how they monetize the data from connected and automated vehicles. In a 2017 KPMG study, 80 percent of the execs who responded agree this data will be the fuel for future business models. Eighty-three percent believe they'll make money off this data. In the process of transforming data into currency, car makers can look at the direct sale of information or look at it to build and strengthen partnerships, reduce risk and increase their financial efficiency.

The Signal Software-Defined Car

Most autonomous vehicle conversations circle around the infotainment aspects of what's happening — ordering pizza while at a stoplight or parking cars with an app. Underlying these discussions is proof that consumers are overlaying their expectations about how they interact with the technology in their car with what they experience with the smartphone industry.

The same technology convergence we've seen with smartphones is beginning to infiltrate the automotive industry — but at a much faster pace. The hardware will make way for software to integrate new technologies, creating an automotive ecosystem that's closely integrated over the next decade. The car of the future will resemble a smartphone not necessarily in function, but rather from the standpoint that it will depend on a standardized software platform — a common operating system through which consumers can "program" their car while still meeting requirements for safety certification, software security and data privacy.

As Senior Vice President and Co-Head of BlackBerry Technology Solutions, John Wall's responsibilities include planning, design and development of QNX Software Systems, Certicom and Paratek products and the direction of its engineering services programs.

SECTION 2

Next Generation Vehicle Architectures

Grant Courville, *Vice President, Products and Strategy*
BlackBerry QNX

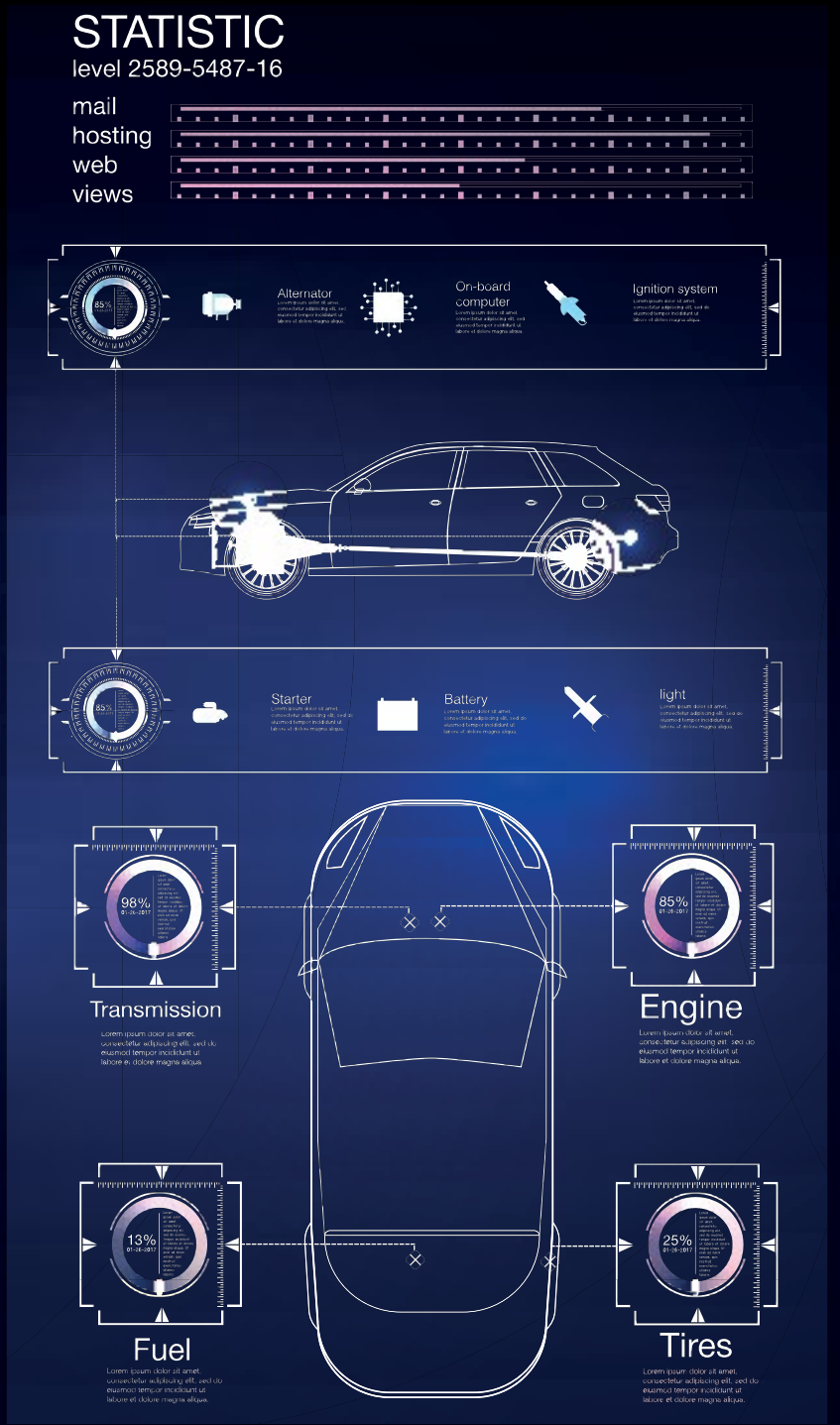
Automakers are redesigning the electronics in the car to address emerging transportation trends and consumer expectations. Years ago, nearly anyone interested in doing basic diagnostics and repair on their own car could do the job. Now it requires technical sophistication, specialized equipment and computer know-how to keep up with the sophistication of how far the technology has evolved. Cars have transitioned from a focus on horsepower and engine size to advanced safety systems and connectivity driven by software.

As the face of the auto industry shifts toward more sophisticated features and autonomous driving, it's time to recognize cars as complex computer systems with hundreds of touchpoints. Today's vehicles are equipped with hundreds of processors that control everything from a car's safety systems to steering, acceleration and more. This means vulnerabilities in the software of a car can put the physical safety of the vehicle's occupants and others at risk. And a majority of the industry is reacting to this.

The creation of the Automotive Information Sharing and Analysis Center (Auto-ISAC), development of key cybersecurity roles within manufacturers and suppliers, the widespread adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and consensus on 'best practices' to follow are all positive steps from an industry determined to protect its customers. It's this potential for access that presents new opportunities for efficiencies and advances in safety systems but also introduces new security risks.

In this move from hardware- to software-defined automobiles, the overall makeup is changing. It is estimated that software represents 10 percent of overall vehicle content today for a large car. However, the average share is expected to grow to 30 percent by 2030.[16]

We see this trend in the models that automakers are getting ready to roll off the line. Audi's new e-tron® electric vehicle offers feature on demand (FOD). The company will offer customers a choice of features that they can buy, after the vehicle is delivered, in multiple formats.[17] BMW's adoption of ethernet means its fifth generation 7 Series takes only 20 minutes to upload 1 Gb of data, compared with 10 hours to handle 81 Mb in its previous model.[18] Jaguar® XJ and Volkswagen® Passat now use ethernet as well.[19]



SECTION 2

Rethinking Automotive Architecture

The McKinsey Center for the Future of Mobility recently published a report called *Rethinking Car Software and Electronics Architecture*. This research and McKinsey's insights provide an excellent window into what we can expect for the entire auto industry as we make the transition from hardware to software. I'd like to talk about four of the points that I find most relevant to the future of electrical and electronic architecture.

The Consolidation of ECUs

As cars gain complexity, so does their internal communication systems. In the past, if an automaker wanted to add a new feature — automatic door locks, speed control, electric power steering, etc. — engineers designed a new system to control each feature. These systems, or electronic control units (ECUs), control one or more of the electronic systems or subsystems in a vehicle.

As drivers expect more and more features in their cars, such as infotainment, telematics and advanced driver assistance systems (ADAS), the number of ECUs has increased dramatically — a single luxury model vehicle may have as many as 150 ECUs.[20] The new electric and electronic features being added has created a large increase in the amount of cabling in vehicles, adding weight, complexity and cost.

For automakers, this creates a dilemma. Rolling out new features and enhancing the driver experience means adding ever-more ECUs. The industry has seen a spike in the numbers as consumer demand increases for more safety features, connectivity and, of course, smartphone-like consumer features. Just as we've witnessed the adoption of common software platforms (operating systems) in the mobile phone industry, the same dynamic is happening in the automotive industry.

Now, automakers are looking to consolidate the capabilities of multiple ECUs into a much smaller number of high-performance systems. New electronic architectures are emerging to help manage cost, power consumption and weight. We're seeing this first in the advent of the digital cockpit. For example, BlackBerry and DENSO recently announced one of the world's first integrated digital cockpit platforms using QNX® Hypervisor (virtualization) technology in SUBARU's latest vehicles. In future vehicles, you will see ECU consolidation where multiple discrete ECUs will be combined into a very small number of high-performance systems called domain controllers, area controllers or zone controllers.[21]

Photo source: BlackBerry.

The consolidation of ECUs is the most evident in the digital cockpit.

Smarter Sensors

With the emergence of advanced driver-assisted systems (ADAS), semi-autonomous and eventual fully autonomous vehicles, there's an accompanying need for more intelligent sensors. The automotive sensor market is expected to expand over the next few years, approaching $44.2 billion by 2026.[22]

Sensors are becoming vital and affect the entire makeup of a car. The increased number of sensors and their technical capabilities will affect the cost as well as the complexity. From a cost perspective, the tradeoff comes in the form of greater safety. Cameras and radar and other sensor technologies are already in use, and automakers will soon be adding 3D LiDAR.[23] Automated drive features will now have more "eyes and ears," which increases situational awareness and the ability to act on information. Drivers, passengers and other users of roadways (vulnerable road users (VRUs)) all become safer.

Automakers are running out of bandwidth, and the amount of wiring and associated weight and cost of copper (wiring) is driving the adoption of ethernet. BMW was the first automaker to use automotive-grade ethernet, which can carry 100 megabits of data per second.[24] The company's X5 SUV uses a setup from Broadcom Corp. for its surround-view camera.[25] Both the Jaguar XJ and Volkswagen Passat now use ethernet as well. When it comes to network speed, there's no comparison. The fourth-generation BMW 7 Series uploaded 81 Mb of data in 10 hours. But thanks to ethernet, the fifth generation 7 Series took only 20 minutes to upload 1 GB of data.[26] Electronic component manufacturer Molex offers a 10 Gbps automotive ethernet platform.[27] We also see CAN bus with a higher potential

through-put to run a gigabit ethernet, which means they can leverage proven IT technology. This shows how effective ethernet technology is in automotive to manage the vast levels of data required.

Connecting multiple-domain controllers by ethernet instead of the traditional CAN bus will allow high-speed and reliable connections that can leverage proven secure protocols (IPSec). It also helps manufacturers reduce connectivity costs by up to 80 percent and cabling weight by up to 30 percent. This provides a cost-effective, scalable solution to the increasingly connected car.

This is not to say that today's automotive network or connectivity technologies will disappear. In vehicles today, you will find CAN, LIN, MOST, Flexray connectivity technologies. Looking to the future vehicle architectures, these will remain in place although for anything high-speed, they will be replaced by ethernet and IP-based protocols and as mentioned earlier, the number of ECUs (nodes) that are interconnected will be reduced.

Updatable Components

Today, when car owners need an update to their vehicle's software, they typically have to take their vehicle to a dealership or download updates on their home computer USB drive and the update is performed manually. This approach is inefficient, inconvenient and comes with its faults. If the driver doesn't have time to go to a dealer or perform the home computer download, they don't get the recommended updates and could risk security and/or safety vulnerabilities. In fact, in 2018 almost 18 million vehicles were affected by software and electronic recalls — up from 2.5 million in 2017.[28]

Now, many automakers have the ability to deliver updates and upgrades over the air (OTA) — similar to how they're done with a smartphone. As long as your phone is turned on, updates can be delivered anytime to wherever you are in the world. With a robust and reliable automotive OTA service, software can be delivered securely and safely to cars in the same way. They can handle issues related to software recall, security updates, and new features and enhancements. Because of the flexibility in delivery, updates can be delivered while the car's in the garage and owner is asleep in bed.

While Tesla has offered this to owners for several years, Ford and GM have announced that some of their 2020 models will accommodate OTA updates. They'll use the technology to deliver upgrades with new features or fix faulty software remotely.[29] This is a big step in the comfort level of mainstream automakers from just a few years ago. Mercedes-Benz has offered OTA updates since 2012 for non-critical infotainment features and Volvo followed suit in 2015. These included things such as navigation map updates and sound system changes.[30]

Making The Transition From Hardware First To Software First

Automakers have come to the realization that the future differentiation and value in the car will be heavily dependent on software. The car is quickly moving from being hardware-defined to being software-defined and, along with this shift, there is a need to adopt a software "platform" approach. This software "platform" approach will allow for more rapid innovation and greater scale. This will provide on-demand car-centric applications such as safety/ADAS features, suspension features, engine features and more. This is part of the value that will be unlocked by automakers for the consumer. A good analogy is the mobile phone industry. Just as we've witnessed the adoption of common software platforms (operating systems) in the mobile phone industry, the same dynamic will be happening in the automotive industry except we all know that the safety, security and reliability needs associated with cars far exceeds that of any mobile phone.

In addition to adopting a safe, secure and reliable software platform, there is also a desire to adopt more of a "Service Oriented Architecture" (SOA) whereby the underlying hardware, sensors and other components and capabilities in the vehicle will be completely abstracted from the higher-level (e.g. application) software. It's this kind of advanced software design and architecture that will truly unlock the game-changing value and associated business models that the automakers are counting on.

Some of the changes noted above are already starting to happen in vehicles (e.g. OTA) while things like wholesale in-vehicle architecture and network changes will take many years to materialize. Consumer expectations and the ACES (autonomous, connected, electric and shared) trends are behind the appetite for change in the automotive industry and status quo is no longer an option. The disruption is well underway, and this presents tremendous opportunities for traditional automotive companies and new entrants alike.

The challenge for the industry is to deliver the highly sophisticated driving experience people want while also ensuring that safety, security and reliably are never compromised along the way.

As the Vice President, Products and Strategy at BlackBerry QNX, Grant Courville is responsible for setting and executing the company's global product strategy for delivering safe, secure and reliable software platform technology.

SECTION 2

Roadblocks and Pathways to the Adoption of Vehicle Electrification

Dr. Austin Brown , *Executive Director*
University of California, Davis Policy Institute for Energy, Environment, and the Economy

Two decades ago, electric vehicles (EVs) were viewed as novelties. Today, with every major automaker working to go electric,[31] EVs are viable and ever-more attractive alternatives to gas-powered cars. Rapidly increasing investment in EVs reflects the substantial benefits EVs have to offer. For individuals, EVs are cheaper to own and maintain,[32] quieter to operate[33] and often provide a better driving experience[34] than gas-powered cars. For society, EVs help improve local air quality and reduce greenhouse-gas emissions.[35]

There is a great deal of uncertainty about how EVs will continue to evolve. It's hard to predict how quickly consumers will adopt EVs and how adoption will affect the electric grid. And while we know that EVs generate fewer emissions on average than gas-powered vehicles,[36] it's hard to predict what the net environmental impact will be. If they are driven frequently and rely on an electric grid powered by fossil fuels, net environmental impacts will be much greater than if they are driven only on occasion and rely on a grid powered by renewable energy.

Fortunately, we're in control of our own destiny. We don't have to wait and see what the future will hold—we can put rules and incentives in place now to ensure that EV deployment positively affects the environment, the economy and social equality. Indeed, proactive public policy is the most effective tool we have to steer EVs towards the best possible future.

Vehicle Electrification Is Poised To Take Off

Changing transportation technology on a broad scale is difficult. Risk-averse manufacturers, regulators and consumers are often reluctant to embrace new innovations. And the slow scale of fleet turnover (the average light-duty vehicle remains in service[37] for more than a decade) means that even once an innovation gains acceptance, it takes time for it to become ubiquitous in cars on the road. The rate of change is even slower when an innovation demands changes to transportation infrastructure as well as to individual vehicles. Note that it was

SECTION 2

nearly half a century[38] before cars and tractors fully displaced horses from roads and farms. Shifting to automobiles required new roads and fueling stations, which simply took time to build.

So we shouldn't be surprised that EVs only account for less than 2 percent of total U.S. car sales. Critics may point to this miniscule fraction as evidence that EVs are impractical for most consumers. The truth is that sales are more or less what we might expect them to be given where we are on the EV technological timeline. EVs weren't even commercially available a decade ago. As the variety of models available for purchase increases and networks of chargers are built out, sales have the potential to grow quickly. This potential is backed by commitments to vehicle electrification from multiple major automakers and national governments. In the past several years, we've seen the following (note that this list is representative, not comprehensive):

- Toyota set a goal to get half of its global sales from electrified vehicles by 2030—then pushed that target up[39] five years to 2025.
- Ford Motor Company announced it would invest $4.5 billion in EVs and produce 13 new EV models by 2020—then ramped that up[40] to $11 billion and 40 new models by 2022.
- Nissan, Mitsubishi and Renault partnered[41] to invest $11.5 billion in EV technology and launch 12 new all-electric vehicles by 2022.
- Volkswagen plans to phase out combustion engines entirely,[42] introducing its last generation of non-electric vehicles in 2026.
- Honda will only sell electric and hybrid vehicles in Europe[43] beginning in 2022.
- Norway announced a goal[44] for all new cars sold in the country to be electric by 2025. France, the United Kingdom and the State of California have announced goals to achieve the same by 2040.
- China has set a goal[45] for 20 percent of new car sales to be electric by 2025.
- British Columbia's Zero-Emission Vehicles Act (ZEVA) will require[46] all light-duty vehicles sold in the province to be zero-emission vehicles by 2040.

Tackling Negative Perceptions

This isn't to say that widespread vehicle electrification is a foregone conclusion. There are still barriers to overcome. One of the largest is overcoming negative perceptions of EVs.

A 2019 poll conducted by Morning Consult[47] found that concerns over range and price are the biggest deterrents for consumers considering EVs. More than 60 percent of drivers flagged range anxiety—the fear among drivers that an EV might run out of power before reaching their destination—and high upfront purchase costs as concerns. The Morning Consult poll also found that lack of variety in the EV marketplace is a problem. While small- and mid-size EVs have proliferated, there are very few electric SUVs, minivans and pickup trucks available for purchase.

The good news is that there are ready answers to consumer questions. EV range isn't as big of a problem as it might seem. The average driver travels just 29 miles by car each day[48]—a distance that can be easily covered by any EV. There are also multiple plug-in hybrid electric models as well as a growing number of high-range all-electric models[49] for consumers with higher driving needs. The average sticker price of a new EV is higher than the average sticker price of a new gas-powered vehicle, but EV prices are coming down.[50] Many federal and state incentives exist to alleviate high upfront costs in the meantime. High EV sticker prices are also offset by lower lifetime fuel and maintenance costs.

When it comes to variety, consumers can take heart that future EVs will likely meet or surpass all of the performance needs of today's gas-powered vehicles. Ford Motor Company, for instance, is actively working on an electric version of its top-selling F-150 pickup truck. An electric F-150 prototype was able to tow more than a million pounds[51], blowing the top-performing gas-powered F-150 (which can only tow 13,200 pounds[52]) out of the water.

A 2019 poll conducted by Morning Consult found that concerns over range and price are the biggest deterrents for consumers considering EVs.

Other companies are making their own bold claims when it comes to electric trucks. Rivian, a Michigan-based automaker, is scheduled to launch[53] an electric pickup and an electric SUV over the next two years. The Rivian R1T truck is expected to have a range of more than 400 miles and boasts the acceleration times comparable with those of a supercar.[54] Arizona-based automaker Atlis is working on an electric truck[55] designed to directly compete with diesel-powered trucks on range, price and performance. Given that light trucks account for about two-thirds of vehicle sales in the United States, fulfillment of even a subset of these claims will represent a real turning point in the EV market.

SECTION 2

Electrification of SUVs and minivans is also underway. Some electric SUVs are already available from automakers including Tesla, Volvo, Audi, Jaguar and BMW. Additional models are just around the corner.[56] While only one electric minivan—the Chrysler Pacifica hybrid—is available for purchase today, Mercedes-Benz[57] and Chrysler[58] are both expected to start producing all-electric minivans in the next year or two. The sticker price of most electric SUVs is currently quite a bit higher than the sticker price of their gas-powered counterparts, and the same will likely be true for electric minivans as well. But prices could drop quickly as technology for larger EVs matures.

Synergies With "New Mobility"

Electrification isn't the only thing shaking up transportation. Automation and sharing are proving to be just as disruptive. Each development is significant in its own right and when combined, these "3 Revolutions" of transportation[59] are even more powerful than the sum of their parts.

Consider, for instance, a couple ready to buy their first new car together. A small, mid-range EV would suit the couple's needs—for grocery shopping, trips around town, a 30-minute commute to and from work—90 percent of the time. But unable to afford two cars, the couple feels they have no choice but to buy a larger, gas-powered car that can also accommodate the 10 percent of the time they want to drive into the mountains for a hike, visit the in-laws a few hours away or move something big and bulky.

Automation and sharing could make it much more feasible to go electric by helping fill the 10 percent gap. It's more realistic to expect owners of mid-range EVs to rent a car for longer trips if rental cars can travel to owners' homes for pick-up and back to the rental-car facility for drop-off. The emergence of companies like Turo, Zipcar and GetAround[60] indicates that there is demand for alternatives to traditional rental-car counters. The availability of car-sharing services further decreases pressure on consumers to buy a car that can meet all of their needs all the time. If our hypothetical couple could rely on a truck-sharing service[61] for those inevitable IKEA runs, an EV might not seem like such an impractical buy after all.

The "3 Revolutions" of transportation may even present opportunities to go a step further and rethink vehicle ownership from the ground up. If automation and sharing make it easy and cheap for people in all communities to request all types of vehicles on demand, it may no longer make sense for individuals to invest large sums of money into buying and maintaining a car that they use only infrequently.

Electrification isn't the only thing shaking up transportation. Automation and sharing are proving to be just as disruptive.

SECTION 2

People might forego individually owned vehicles in favor of subscription-based services that enable access to bikes, scooters, transit, cars and other mobility options through a single platform. Think Netflix or Hulu for transportation. Or people might choose to go in with their neighbors on a long-range, high-performance EV that would be too expensive to purchase individually but makes sense to share among a small group. Think timeshare for cars.

The upshot is clear. Once we break away from the conventional vehicle-ownership paradigm that has dominated the transportation sector for decades, a world of exciting transportation possibilities presents itself.

The Role Of Public Policy

Whether or not we realize any of these possibilities depends largely on the shape of the policy landscape. The transition to EVs is already underway, supported by incentives recognizing the benefits EVs deliver to society. An important next step is to think about how we restructure and/or expand EV incentives to prioritize electrification where it is needed most.

One of those areas is ridesharing. Vehicles serving transportation network companies (TNCs) like Uber and Lyft travel more miles[62] on average than personally owned vehicles—up to an average of 180 miles per day for the former versus 38 miles for the latter in California. This means that electrifying one TNC fleet vehicle yields much larger emissions savings than electrifying one personally owned vehicle. But TNC drivers don't receive disproportionately larger incentives for buying an EV. Policymakers could consider restructuring state and federal EV sales rebates and tax exemptions for drivers who dedicate a set percentage of time or vehicle-miles traveled to TNC service.

Policymakers could also set mandates for TNC companies to electrify a certain percentage of their fleets: whether by providing EV rentals to drivers,[63] increasing the percentage of gross revenue that EV drivers get to keep or some other creative solution. Uber provides an example of what such a solution might look like. In January 2019, Uber added a "clean-air fee" of 1 pence per mile to Uber rides taken in the London area. The money raised goes into a pool that Uber uses to help riders upgrade to and maintain EVs and support other clean air initiatives. Once drivers have an EV, the Clean Air Fee can then be put toward on-going vehicle costs. Uber likely selected London for this experiment because of upcoming restrictions to gas-powered vehicles in the city, demonstrating the importance of policy leadership to get companies to change.

Policymakers also have to think about expanding EV infrastructure. Even now, with EVs accounting for only a small share of vehicles on the road, a shortage of EV chargers is leading to "charger rage"[64] in some major urban centers. Some places simply don't have EV chargers available at all, making it nearly impossible for anyone to go electric. Charger shortages are particularly problematic for those living in apartments, who can't install chargers at home. Government could lower financial barriers to charger installation by matching some or all of the funds invested in charging networks by TNCs, utilities, charging companies and property owners. Government may also have to assume sole responsibility for funding chargers in remote locations, low-income communities and other areas where the private sector is unlikely to fully meet public demand.

The Bottom Line

EVs are totally indispensable if we are to avoid the worst effects of climate change. They can also deliver better customer experiences, make travel cheaper, and improve the livability of our cities and communities. The bottom line is that electrifying transportation is unquestionably a goal worth pursuing.

The outstanding question is how quickly our transportation system can change over. Consumers are gradually starting to see EVs as viable alternatives to gas-powered cars, and major automakers are investing billions into new EV technology and models. But without strong policies pushing electrification along, the transition won't happen fast enough. It was fine to wait 50 years before gas-powered cars fully displaced horses. But with the climate crisis upon us, we don't have 50 years to spare to let electrification proceed at its own pace. Policymakers need to get serious—about imposing aggressive EV mandates, building the infrastructure and funding incentives. Policymakers also need to work with transportation experts and transportation companies to develop strategies for optimizing the simultaneous evolution of electric, automated and shared vehicles. By taking strong, thoughtful action now, we can realize a fully decarbonized, equitable transportation system in the near future. That prospect is electrifying.

Dr. Austin Brown is Executive Director of the Policy Institute for Energy, Environment, and the Economy and an Adjunct Professor of Civil and Environmental Engineering at the University of California, Davis.

SECTION 3

Bottlenecks to Change

SECTION 3

The Elephant in the Room: Shifting Culture from Competition to Collaboration

Faye Francy, *Executive Director*
Automotive-Information Sharing and Analysis Center (ISAC)

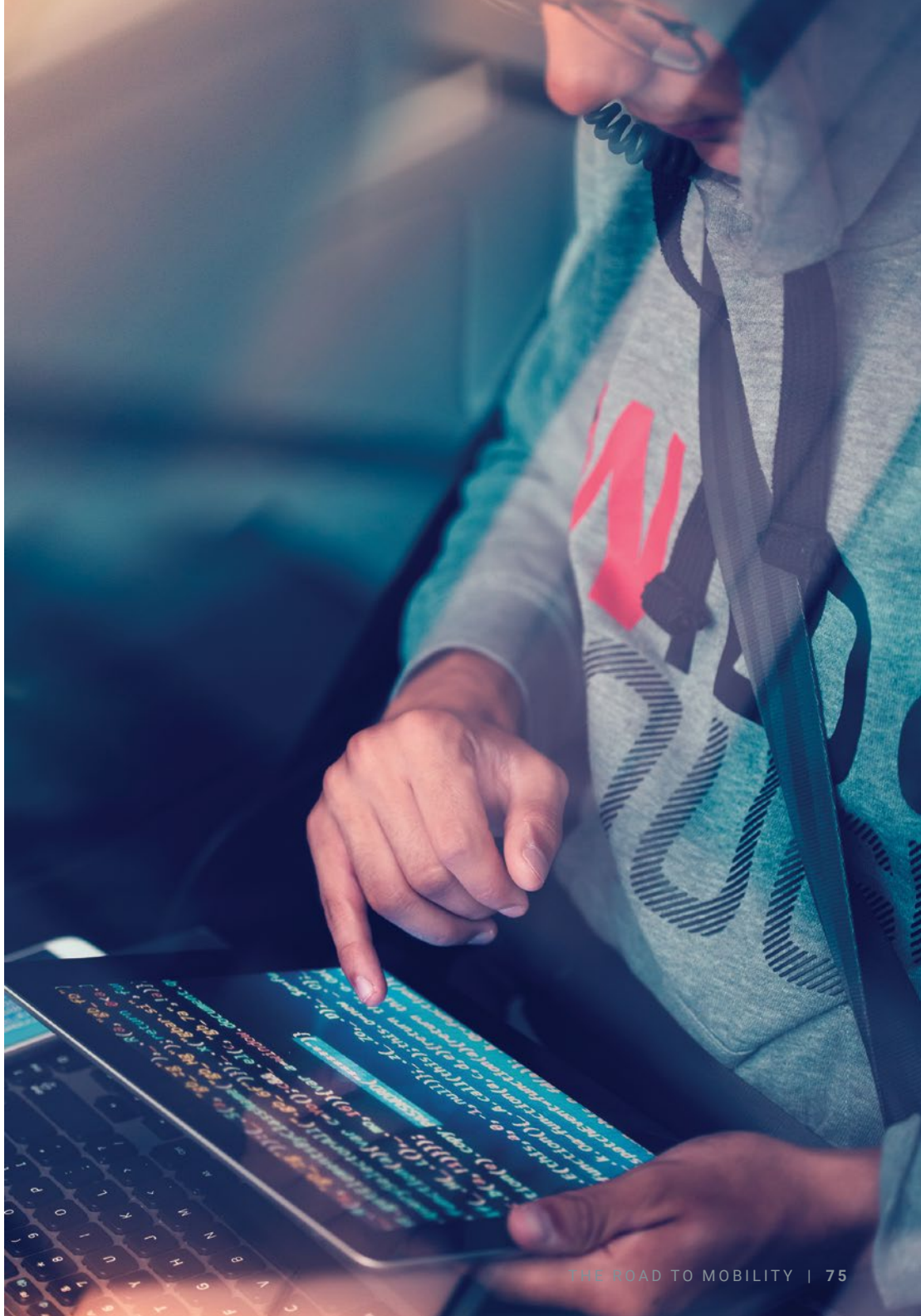
We live in exciting times, and tomorrow's world of transportation has everyone's attention. Automakers are working hard to develop and release the latest technologies and develop strategic partnerships to stay ahead of the competition. Dealerships look at how to woo forward-thinking customers and keep their OEM's brand top of mind. In the midst of it all, consumers are spinning as they try to comprehend the pace of change and what it means to them. The deluge of information about connected and autonomous vehicles brings both excitement and trepidation as people comprehend how it all affects the safety and security of their lives.

In all of the churn, there's an unspoken relationship between automakers, dealers, suppliers and customers. OEMs will always remain competitors. But now they are reexamining the relationships between these groups and considering how the future of transportation changes the entrenched dynamics of the past.

Think of the consequences to consumers — what might happen if their key fob is "hacked" and the auto is stolen? Everyone understands that safety from all directions is paramount. But the public won't move toward connected and autonomous vehicles with blind faith. If they do and they see something bad can happen, they'll quickly end up losing trust.

As a nonprofit organization, the Automotive-Information Sharing and Analysis Center (Auto-ISAC) serves as a platform to understand the efficiencies and risks that come as we move toward connected and autonomous vehicles. We're built on a foundation of collaboration and information sharing to strengthen the industry's capability and capacity to detect, prevent, respond to and mitigate disruptions that happen with connected vehicles and the infrastructures that support them.

In order to create more resiliency, the automotive industry is working together, building trust so we all can ensure the safety and security of all consumers. To successfully do this, we must place our focus on three areas.



SECTION 3

1. Cybersecurity

As cars and other forms of transportation increasingly incorporate in-vehicle computer systems, cybersecurity has become one of the industry's top priorities. As a 100-year-old mechanically driven industry, automakers were, for years, focused on safety. However, now that we've entered the age of IoT — Internet of Threats as I define it — we must become vigilant about what we do and how. Doing so means looking at security from the outside-in, starting with a global perspective and the consequences from the broader industry, then working back into the perspective of individual companies.

Cybersecurity is an asymmetric threat. This untraditional method of warfare puts us up against situations we can't predict because we don't have a full understanding of what it involves or how it's launched. Cybersecurity brings constant and emerging perils. Just as you close the door on one attack, a hacker opens a different door or window and enters somewhere else.

These threat actors are ahead of us on the learning curve. They can get through a firewall or intrusion detection system (IDS), the industry learns how to stop them and then the attackers are off to something else. The solution requires vigilance and monitoring on the part of the entire automotive industry to determine whether a system remains secure or has been compromised.

Cybersecurity brings constant and emerging perils. Just as you close the door on one attack, a hacker opens a different door or window and enters somewhere else.

For automakers who've suffered an attack, the question to resolve is this: How do I know that the vehicle architecture is still safe and secure? We discover new vulnerabilities daily, which means OEMs must constantly reexamine their architecture to make sure there's no impact or negative ramifications. This requires vigilance yet makes it more challenging for the industry from a resource and response-time perspective. Just as you think you have the issue resolved, the attackers find another door through in which to enter. The next step, then, is to contain or expel them.

The ability to stay ahead of these attacks and keep safety and security at the forefront of what we deliver to consumers requires all of us to rethink the relationships we have as competitors and open the door to greater collaboration.

SECTION 3

2. Healthy Collaboration

No industry can succeed without a common goal. For the automotive industry, we began working together four years ago to identify threats sooner and share solutions to enhance vehicle cybersecurity. Everything we do — whether it's the design of a new vehicle, manufacturing, or how it's sold and serviced — requires us to think through the smallest detail to ensure that we've embedded the appropriate safety and security. As connections along the supply chain and the vehicle itself integrate, we must think of the potential impact of that data and how we handle protocols for its use.

In order to understand how to counter threats, we look at this through the eyes of others. Threat actors collaborate and share information all over the world. They give each other advice, put tools on the dark web and post passwords — they're committed to advancing the knowledge and skills of the greater community. The automotive industry, on the other hand, is new to this type of collaboration because of our competitive and legal structures. There's an ever-present fear of retribution or financial ramifications.

Everything we do — whether it's the design of a new vehicle, manufacturing, or how it's sold and serviced — requires us to think through the smallest detail to ensure that we've embedded the appropriate safety and security.

As automakers and tiered suppliers have transparent discussions amongst themselves, it leads to honest conversations with consumers and greater trust. Working together, we are able to identify and address potential threats and the impact they can have. For example, should an attack happen that affects traffic flow into a major metropolitan area, the entire urban center could be held hostage. But, as the automotive industry proactively shares information, it will be better equipped to head off potential attacks that have wide-spread impact.

We can learn lessons from other industries that have already taken steps in this direction. For example, when Boeing's 747 planes were used in the attacks on the World Trade Center, the entire airline industry was affected, taking a decade to recover. During this time, they collaborated in order to improve the safety and security of the aviation industry and rebuild consumer trust.

The automotive industry learned from aviation and other sectors in transportation how to share information and mitigate the risk of a "cyber 9/11". To prevent a tragedy at this scale of the 9/11 attacks requires changing our mindset from "Did my brand get attacked?" to "Did my industry get attacked?" By starting with mitigation techniques, we eventually discover greater efficiencies that will move everyone farther, faster. This is especially true as we look at machine learning and artificial intelligence. What we can learn in a few years through shared data would take us 20 years if each OEM tried to go it alone.

3. Build Resiliency

The last part of the equation is our ability to build resiliency. Just like the policies, procedures and plans that are ready-to-use when a recall is issued, we must prepare for these ahead of time in case of a cybersecurity issue. Resiliency comes down to understanding the crisis communication and actions that needs to be in place — how do I respond and to whom — and then practice the plan through drills and tabletops. This industry is holding tabletop exercises to ensure preparation for cyber-security situations and communications are understood, and we are able respond in an efficient and effective manner.

Tackling the Elephant

Automakers have used safety as a distinguishing brand feature for years, and cybersecurity now has become a part of the message. However, as the industry works to successfully weather the impact of an inevitable attack, we need to collectively create best practices that will guide risk management at the product level and further enhance the security and resiliency for the whole of industry. By shifting the culture from competition to collaboration, great things will happen for everyone.

As the Executive Director of the Automotive-Information Sharing and Analysis Center, Faye Francy serves the global automotive industry through strategic leadership. This fosters collaboration for mitigating the risks of a cyber-attack.

SECTION 3

Challenges to Smart Mobility and Smart Cities

Roger C. Lanctot, *Director, Connected Mobility & Global Automotive Practice*
Strategy Analytics

Wireless technology is not new to the transportation industry. What is new is the growing recognition that connecting citizens and the means of transportation, whatever it may be, contains the promise of saved lives, reduced emissions, and enhanced and efficient social mobility.

Innovators, regulators, and legislators are looking to connectivity to unlock latent value propositions in managing transportation systems and people via connectivity — an Internet of transportation. This IoT holds extraordinary promise but there are tremendous unresolved obstacles in the form of existing consumer behavior, business models, cybersecurity and privacy issues, regulatory vision, funding and technology.

Consumer Behavior

Consumers surveyed by Strategy Analytics in Europe, North America and China report four key factors around their transportation decision making behavior: availability, cost, time and experience. Availability is the most obvious factor — with the ease of access determining a lot of basic transportation decision making between public and private transportation options. Related to availability is the ease of inter-connection between different modes of transportation.

Cost is a key motivator for the use of public transport and ride hailing services versus relying on privately owned vehicles and the related sometimes onerous costs of ownership. Parking costs at destination and congestion charging are influential variables in this context. Personal experience, too, applies including first and last-mile convenience, comfort factors, vehicle condition and safety.

Business Models

What is new in the realm of connected transportation is the onset of connected solutions ranging from autonomous and electric vehicles, shared cars, ride hailing, to the full range of micromobility options. Business models are essential to driving consumer behavior and generally revolve around the length of journeys and the cost and ease of use of different transportation modes.

SECTION 3

The key common denominator among all of these emerging transportation choices is the app-driven side of the user interface. Consumer preferences in this app-driven environment are determined by cost, convenience and, above all, ease of use.

Ride hailing has emerged as the pre-eminent transportation mode of the future, muscling aside ubiquitous taxis with discounted fares and easy-to-use apps. Car sharing, too, has sought to tap into the app access advantage with some limited success.

The difference in the proliferation of ride hailing — with millions of drivers and tens of billions of dollars in revenue — compared to car sharing — with fewer than 300,000 cars globally and $4B in revenue in 2018 is stark. Ride hailing continues to shake up transportation networks globally while car sharing is seeking to find its natural place in the transportation mix.

BTC Worldwide Estimated Metrics

Total Revenue: $3,983B USD
The average user spends about $118.94 USD per year on car-sharing

Total Registered Users: 33.48M People
On average, there are about 136 users for every one shared vehicle

Total Vehicles: 250,000 Cars
Each vehicle brings in a little over $16,000 USD per year on average

Source: Strategy Analytics

Micromobility, meanwhile, has taken cities by storm — with regulators struggling to cope with the challenge of managing a growing onslaught of two-wheeled vehicles. Scooters, in particular, have established a permanent presence in a growing number of cities globally as municipal authorities move increasingly to accommodate what is seen as a low cost, low emission transportation option.

Cybersecurity And Privacy

Deploying connected transportation technology increasingly requires added attention to cybersecurity hygiene. Vehicle and customer data theft have raised consumer and legislative alarm as have potential and actual violations of privacy.

Historically, auto makers have relied on the marginal interest of hackers in penetrating automobiles combined with the perceived difficulty under the rubric of "security by obscurity." The conventional wisdom dictated that no one really needed to worry about cars as a hacking target because the perception was that cars were sufficiently secure and hackers were sufficiently uninterested.

We now know that not only are cars not sufficiently secure, they are a potentially rich source of personal data and an attack vector via which car companies might actually be penetrated. Standards and regulations have now been adopted globally requiring that auto makers work cybersecurity into their design processes, production lines and dealer service bays. The industry is formally in a full-blown scramble to comply and suppliers have rushed into the breech with a wide range of solutions to tackle the multi-faceted challenge.

We now know that not only are cars not sufficiently secure, they are a potentially rich source of personal data and an attack vector via which car companies might actually be penetrated.

Success in connected transportation is seen as requiring critical cybersecurity decision making motivated by regulatory requirements. In fact, while auto makers have responded, even infrastructure companies are implicated and are working at their own pace to secure their own wireless interfaces. The final note is the fact that the auto industry has come to recognize that there will be no cybersecurity without connectivity.

Privacy, too, is influencing decision making around connecting vehicles for the purposes of enhancing the safe movement of people and goods without compromising personal information or privacy. While some may perceive the passing of Europe's Global Data Protection Regulation (GDPR) and California's passage of the California Consumer Privacy Act have purely local implications, the reality is that both laws have global implications.

Car companies are brushing up their consent management assets and data anonymization algorithms to comply with these new laws. With some proactive decision making and implementation the auto industry may well avoid any slowing data monetization activities resulting from efforts at preserving consumer privacy — even in the context of proliferating driver monitoring systems.

SECTION 3

Regulatory Vision

The main stake that regulators have in the transportation game revolves around mitigating congestion, reducing emissions, and eliminating crash-related injuries and fatalities. Now, more than ever before, connected vehicles offer the promise of leveraging vehicle data to facilitate the avoidance of hazardous conditions along public streets and highways.

With the arrival of ride hailing, though, regulators and legislators are being forced to consider issues of equity and employment policy. These battles have only just begun, but they have forced municipal authorities to reconsider their processes for credentialing transportation service providers in the context of establishing compensation and service delivery equity.

Vulnerable populations must be served equally by all. And the welfare of drivers and passengers alike must be protected.

As much as ride hailing service providers have shaken up regulatory priorities, the rise of micromobility has demanded the attention of legislators. By and large, cities have seen fit to accommodate two-wheeled mobility services with new rules, bike lanes and road diets. Micromobility may be limited to fair-weather periods of operation, but cities see micromobility as an attractive alternative to four-wheeled options.

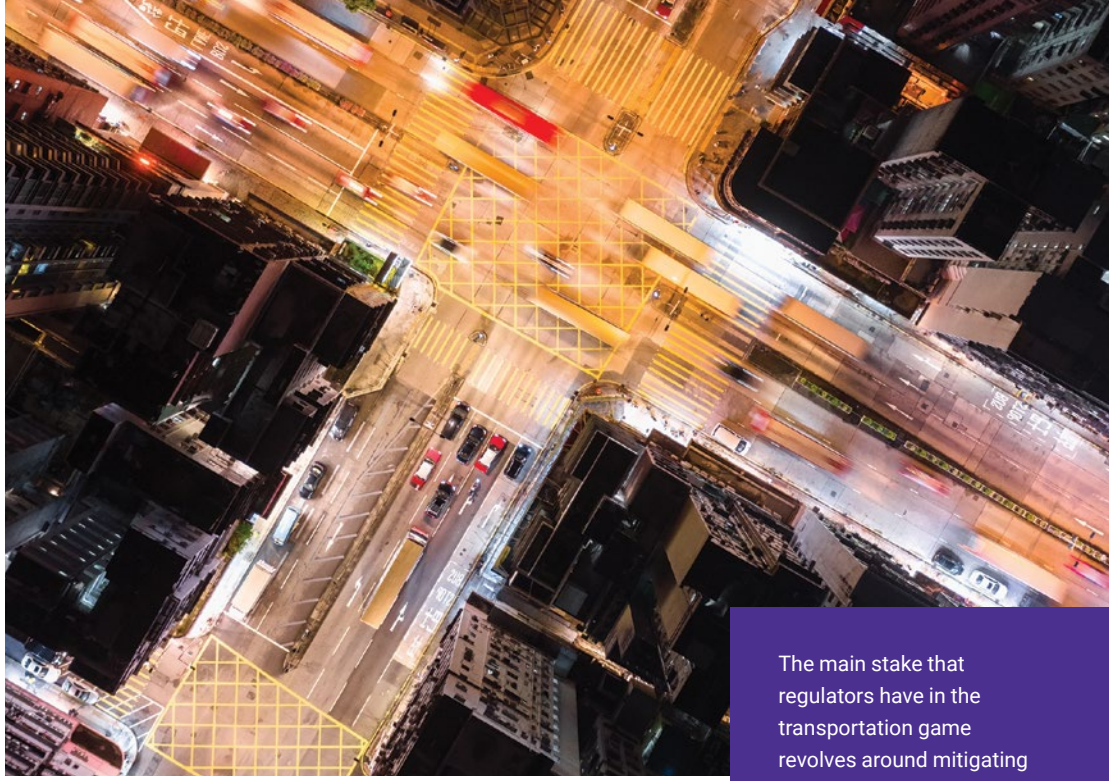
Funding

For the time being, transportation authorities are focusing public transportation investments on traditional targets such as buses, trams and taxis, leaving emerging shared modes of transport to private operators. Municipalities have seen fit to tax service providers. They are increasingly exploring multimodal transportation platforms intended to empower local authorities to manipulate and manage travelers with rewards and incentives.

This nascent process of aggregating transportation in the interest of optimization of available options is still new and driven by conflicting payment platforms and private interests. In the long run, connected multimodal transportation options will come together to form a vision of mobility as a service (MaaS).

MaaS is increasingly seen as a multi-level process defined as follows:

- **Level 0 = no integration of services.** Separate services are provided for different means of transport.



The main stake that regulators have in the transportation game revolves around mitigating congestion, reducing emissions, and eliminating crash-related injuries and fatalities.

- **Level 1 = integration of information.** Travel information is provided through (multi-modal) travel planners, which may or may not include information on routes and costs. Level 1 facilitates the choice regarding the time of day, the route or the mode of transport to be used.
- **Level 2 = integration of finding, booking and payment.** MaaS facilitates the finding, booking and payment of individual trips. Users can find, book and pay for their trip at a single service point (e.g., through an app with a pre-registered credit card).
- **Level 3 = integration of transport services into passes and bundles.** MaaS does not just cover individual travel movements; the service also meets the full daily mobility needs of individuals and families by offering different means of transport through bundles and/or passes. Offers users an alternative covering all their daily mobility requirements. Also constitutes an alternative for individual car ownership.
- **Level 4 = integration of societal goals.** MaaS extends beyond liaising between the demand for and supply of mobility. Supply and demand are now combined with social goals such as reducing the use of cars or promoting liveability in the cities.

SECTION 3

Typology of Mobility-as-a-Service with Levels

4	**Integration of societal goals** Policies, incentives, etc.
3	**Integration of services offered** Building/passes, contracts, etc.
2	**Integration of booking and payment** Each vehicle brings in a little over $16,000 USD per year on average
1	**Integration of information** Multi-modal travel planner, price information
0	**No Integration**

Technology

Connectivity and technology are the factors that are transforming transportation and enabling systems and solutions intended to resolve negative transportation-related exigencies. At the core of the technological change revolutionizing transportation are wireless cellular connections.

Wireless technology is nothing new. General Motors' Onstar system has been available for 23 years. What is new is the ubiquity of wireless connectivity and the growing recognition of the power of data.

Ubiquitous wireless connections mean that trains, buses, cars, taxis and scooters can all be connected and tracked. Tracking means individual vehicles and systems can be optimized and prioritized.

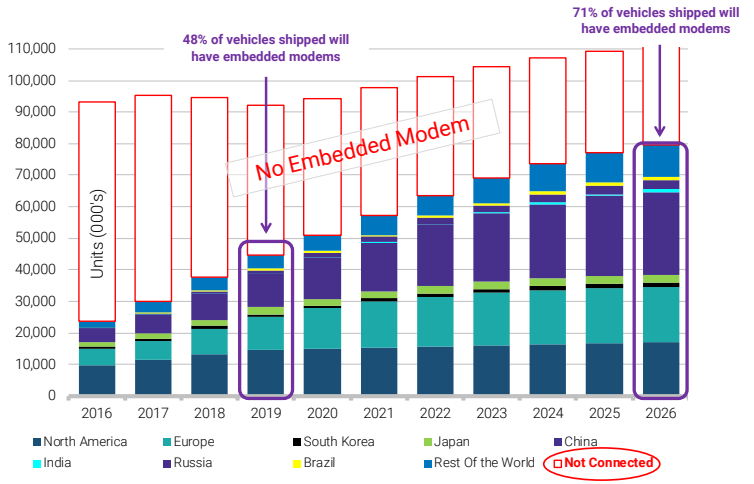
Wireless technology itself is evolving to enable true IoT functionality with vehicles able to communicate with other vehicles, infrastructure and pedestrians. The emergence of C-V2X and, eventually, 5G technology will enable collision avoidance applications built around wireless connections.

Implications

In Europe, the United States, China and around the world, there is a growing recognition that wireless connections in motorized vehicles and mobile devices are creating new opportunities to overcome transportation challenges. Wireless connections are improving vehicle throughput while reducing congestion and collisions.

To reap the full benefits of vehicle connectivity, manufacturers are putting in place embedded systems capable of gathering, aggregating, exchanging and interpreting vehicle data in real time. The next phase spreading around the world is the effort to integrate data from moving vehicles with transportation systems and their related data.

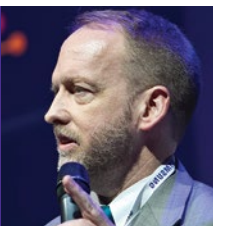
Automotive Embedded Modem Global Annual Shipments



Source: Infotainment & Telematics Service

Efforts such as the European Data Task Force and others are building the on-board and off-board solutions designed to help connected transportation systems to put data to work to simplify and optimize consumer transportation decision making while reducing negative impacts. The transportation networks of the future will be defined and enhanced by advanced hardware, software, and connectivity systems enabling data-driven systems.

Roger Lanctot is an Associate Director in Strategy Analytics' Global Automotive Practice. He draws from his 25 years as an analyst, journalist and consultant in the technology industry to define future trends in automotive safety, powertrain and infotainment systems.



SECTION 3

Keeping Safety at the Forefront of Automotive Advancements

Yi Zheng, *Senior Product Manager and Embedded Software Expert*
BlackBerry QNX

The amount of technology that cars contain has spiked. OEMs have taken big steps to make them safer, smarter and more fun to drive. However, more electronics mean more complex systems. In looking at creating safer vehicles, there are three building blocks for the industry to understand that have a growing impact on trust between consumers and automakers.

The Critical Nature Of Safety

Safety is the mission-critical part of the automotive software system. If we think back to what the term meant 10 to 20 years ago, it was a simple list of things such as seatbelts and ABS. As we look at the safety of cars today, however, it is a completely different picture and serves as the foundation of everything on which we build. Functional safety is now an extremely important part of cars, both in protecting lives and property, and creating a competitive advantage for OEMs and Tier 1 suppliers. It's no longer just about the safety of the vehicles, but about the safety of the software on which they run.

As automakers look at how to move beyond the structure of the vehicle in finding a competitive advantage, software is the new offering. The value of cars is increasingly dependent on the systems that run them. We see this in manufacturers such as Tesla, which offers additional functionalities through software upgrades. As cars become more and more connected, delivering features in this way will become common practice.

Despite its mission-critical nature, software is not a well-understood part of functional safety. ISO 26262 provides an international standard for the level of safety for the functions in electric cars and electrical systems. Published in 2011, it's a recent development in an industry that's more than a century old. ISO 26262 has created a universal yardstick for the functional safety of cars. Yet, even with the

SECTION 3

increased attention and standardization of automotive safety, only one chapter out of 10 is dedicated to software. As a result, the standard provides solid guidance, but falls short of a comprehensive directive for functional safety and software.

As software controls more things in vehicles, it's crucial to address the safety aspect to protect the lives of people. While many functions are simple — rolling up a window, turning on blinkers — there's a growing number of progressively complicated systems — navigation, satellite communications and even the more futuristic ADASH software in which the car is trying to take over the capabilities of the driver. There are few Level 3 or 4 systems on the market today but no Level 5. Before we can take this last step, the industry will require new laws and legislation that cover the functional safety of vehicles and the software behind it.

All of this leads to a conundrum — the increasing use of software has brought us to a point of improved safety. To keep safety intact, we need ways to monitor the software to make sure that it does, in fact, keep drivers safe while reducing liability for OEMs.

Easy To Say, Hard To Do

While focusing on improving the quality of the systems behind the wheel sounds simple, automotive software safety and functionality is a highly specialized field. It often depends on the correct operation of software-based systems built from many different components. Good design requires that these components be isolated from each other on multiple axes, so they don't inadvertently interfere with each other. Delivering successful systems requires a unique expertise across the entire design cycle.

This poses a problem that feels impossible to solve for the industry. OEMs want to build a car with functionally safe software that carefully considers all the hazards and risks a driver may encounter. This leads to the demand for a team of designers who deeply understand what it takes to build safety-critical software. This group of experts, however, doesn't yet exist on staff at automakers.

We can find these experts more easily in the non-imbedded auto space because there are other markets that have a high-demand for this level of safety proficiency. For example, BlackBerry services other groups that are safety critical such the nuclear industry, high-speed trains and robotics. Each of these has functioned under their own governing safety standards for many years. These industries have experts who have an intimate understanding of what it means to build functionally safe software.

For automotive, software is catching up to other industries and its use is quickly increasing. Electronic systems in cars started out with infotainment system and there was nothing life threatening if it failed. There wasn't a need for a rich well of safety-critical engineers like there is today for OEMs to staff emerging auto projects.

Where do we begin to tackle the talent dilemma?

First, we have to be realistic about the time frame in which we can recruit competent experts. As designers and engineers go through their education programs, there's no course or series of classes that address how to design safety-critical software. It's impossible for the auto industry to look at universities as a source for talent that's armed with the skills and expertise for the nuances of the situation. The exception is someone with a Ph.D. in this specialty area. But the time required to turn out these professionals to meet the current level of demand is unrealistic.

If automakers are going to maintain a culture of safety, then they need to extend this mindset into how they build safety critical components. A culture that's serious about safety trains its designers and engineers on a mass scale on any topic related to safety. Secure software functionality is no different.

Producing skilled experts starts with organically growing a core competency. On-the-job exposure through grooming, teaching and training is the surest way to help these budding experts understand what it means to build safety critical systems.

A close second to home-grown expertise is leveraging expertise from other markets. BlackBerry has a strong background in safety because we've been served other safety-critical industries outside of automotive. Our QNX group has a team with a large percentage of engineers who've gone through safety training. Taking advantage of this established expertise can help OEMs and Tier 1 suppliers jump-start progress.

> **A culture that's serious about safety trains its designers and engineers on a mass scale on any topic related to safety. Secure software functionality is no different.**

And the last option is to mandate compliance to safety standards to reinforce that there's no question about a company's commitment to safety. This sends a powerful message both in-house and to customers that you're serious about the safety process. While time-consuming and expensive, this statement definitively sets a company apart from its competitors.

SECTION 3

Potential Solutions

Safety-certifications are complex, and we understand the pain that OEMs are going through. Having pre-certified or pre-assessed software components reduces the time it takes to bring new models to market, their cost and the difficulty of getting certification for the end system. As an industry, this is something we all need to take care of for the safety of people. And it's something that we can all work through together.

As we've worked with customers on various software deployments, we see OEMs looking into a standard that evolves the level of safety set by ISO 26262, and that is ISO 21448. Also called SOTIF (safety of the intended functionality), this standard applies to functionalities that require proper situational awareness so they meet higher standards of safety. While ISO 26262 looks at mitigating risk because of a system failure, ISO 21448 seeks to guarantee the safety of a functionality outside of a fault. It provides guidance on design, verification and validation measures and helps OEMs deliver safety in situations without a system failing.

These are the types of requirements that BlackBerry takes into account when our teams look at the ecosystem of a car and write an operating system for it. For a programmer, writing an OS requires hundreds of thousands of lines of code, which is a significantly complex challenge on its own. However, this seems small compared with an OEM that has responsibility for everything bumper to bumper — wheels, airbags, doors, etc., plus the hardware and software that connects it all together. As software and technology grows more complex, the responsibility of automakers grows broader and deeper.

BlackBerry understands these challenges. Our QNX software sits on an OS that an OEM or Tier 1 supplier has selected, supports functions that run on the OS and becomes embedded in the car. It follows a two-part safety certification:

1 **Product development life cycle.** In looking at the product lifecycle, and given the task of writing a feature for a product, the first question the QNX team asks is, "How do we do it?" Next, we identify the set of agreed upon rules to follow during the development process. This may mean having five people inspect the code and provide comments, or test it and reach 100 percent functionality. As a typical product development lifecycle, this process is second nature for BlackBerry — a company with a mature process and experienced team.

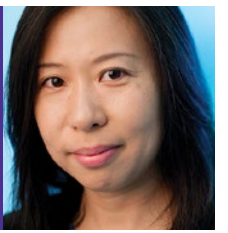
2 **Hazard risk analysis.** This scenario is harder and looks at how the work actually gets done. Take, for example, the OS. It has a scheduler that charts each task to run. Once it finishes with one, it picks another and continues in a linear order. While at first glance this seems low-risk, our QNX team digs into what would happen if it didn't work properly. What's the impact for a car that depends on this? What happens to the scheduler? It sparks an entire range of questions about the safety functions that are to be delivered. These are things that safety standards don't outline how to do, and it prompts many different questions from the middleware company that aren't on the radar of most software company.

It can take years and cost millions of dollars to go through certification. And in the end, approval may be declined. BlackBerry understands these subtleties and takes care of them properly. Our QNX software delivers on both the process and safety features. This lowers complexity and helps OEMs get a better handle on the quality and safety of the final product that ships — which delivers greater safety for everyone involved.

When Failure Is Not An Option

Compliance with ISO 26262 can only take OEMs so far. Which is why BlackBerry has invested so much time developing stringent specifications that support our work. QNX OS helps ease the apprehension automakers have around their lack of safety knowledge and expertise. BlackBerry's mission-critical embedded systems run every day, in every situation, providing utmost safety without failure. Our safety-certified software is the outcome of world-class dedicated professionals serving the auto industry by increasing reliability, shortening time-to-market and reducing development cost.

Yi Zheng is BlackBerry's Product Manager responsible for the safety of products being certified to IEC 61508 SIL3 and security products certified to Common Criteria EAL4+ at QNX Software Systems. She also manages the QNX Neutrino RTOS and the QNX Momentics tool suite.



SECTION 3

Using Artificial Intelligence to Boost Connected Vehicle Security

Ashkan Amiri, *Director, Data Science*
Andrew Walenstein, *Director Of Security Research And Development*
BlackBerry's Advanced Technology Development Labs

Connected devices and artificial intelligence (AI) are big parts of the future. The number of connected devices is growing exponentially and so is AI and its involvement. Among the many devices that bring us convenience, vehicles have a special importance as they touch, both directly and indirectly, many aspects of our lives. The level of dependency we have on the vehicles and the amount of time we spend moving around in them has created a potential market for new ideas and innovative solutions. AI is a big part of this picture.

The most straightforward model of application of AI in vehicles is to treat them as computing nodes. Modern vehicles are, in fact, a "network on wheels" of distributed computers. In a similar fashion, the scenario, just described, would treat a network of connected vehicles as a network of computing nodes.

In this model, everything for which we currently use AI can potentially be translated over and applied in the vehicle. Cybersecurity as an indispensable feature of a network is one important application of AI in connected vehicles.

In this context, some of the AI-for-cybersecurity products that immediately come to mind include:

- User authentication and authorization to detect and prevent their misuse
- Malware and botnet detection to avoid advanced persistent attacks and data loss
- Data loss monitoring and prevention to protect privacy and user information
- Intrusion prevention and detection
- User behavior analysis, for example to detect an impaired or fatigued driver
- Monitoring ECUs and sensory modules to detect misbehaving or defective units
- Monitoring internal networks to ensure the integrity of communications between key components of the vehicle

- Monitoring external communications, such as those between vehicles or between vehicle and cloud server, to identify jamming, denial of service and so forth.

Due to the availability of massive amounts of data and the maturity of data science tools and techniques, making use of the technologies above in vehicles seems within reach. This is assuming, however, that the vehicle manufactures are willing to add the required processing power to enable collecting data and operating these AI-for-cybersecurity technologies.

Due to tight profit margins of vehicle manufacturing, OEMs might not yet consider cybersecurity as a high investment priority. But with millions of connected vehicles being produced every year globally, we'll experience an inevitable shift in priorities.

An important aspect of cybersecurity that often lacks attention is the implications of security risks on safety. An example is a security attack that intervenes with the function of a safety mechanism or one that triggers the mechanism when there is no real need. Imagine an attack in which the integrity of distance measurements is affected, which keeps the vehicle from activating the brakes to avoid collision. Or, an attack on the airbag system so it inflates while driving at a high speed.

Due to tight profit margins of vehicle manufacturing, OEMs might not yet consider cybersecurity as a high investment priority. But with millions of connected vehicles being produced every year globally, we'll experience an inevitable shift in priorities.

As the software footprint in vehicles increases and the internal workings of vehicles become more accessible to the outside world, the attack surface becomes larger. So too, then, do the implications of security risks on safety. Fortunately, it is becoming more widely understood that safety and security are substantially intertwined; in other words, there is no safety without security.

One thing that cannot be expressed enough is that with connected vehicles, safety is no longer an issue that can be handled within individual vehicles. Once a vehicle is connected, it automatically becomes part of a bigger system. At this point, it can receive information and then take physical actions in response. These physical actions may have severe impacts and therefore consequences.

While the most immediate risk is the threat that such physical actions may impose on the safety of individuals, the potential implications could be far greater. Given the number of vehicles on the road, the consequences associated with an event such as a swarm of vehicles being taken over by an adversary could have ramifications only comparable to those of a natural disaster or, even worse, an act of war.

From a completely different perspective, impacts of an attack could go beyond what's immediately visible, such as societal consequences. Imagine journalists, activists, political figures or their loved ones becoming targets of aggression and how it could affect democracy. Or, business leaders besieged the consequences it would have on the world economy.

A network of connected vehicles is an enormous and complex system of sensors and actuators that function within the same environment — similar to human beings. As the number of connected vehicles grow increasingly, so, too, does the complexity of this system. Interactions with the environment could reach a point in which traditional approaches to risk management become futile because of the number of moving parts and infinite space of possibilities.

Consequently, the straightforward models described earlier are not sustainable. Instead, a holistic approach is required to ensure safety, and AI is a technology that can make that approach feasible at scale.

Ashkan Amiri is a Director of Data Science within BlackBerry's Advanced Technology Development Labs, where he leads the development of artificial intelligence and machine learning solutions.

Andrew Walenstein is the Director of Security Research and Development and leads the Advanced Research and University Collaborations group within BlackBerry's Advanced Technology Development Labs. Previously, he was a professor of computer science at the University of Louisiana at Lafayette.

SECTION 3

Underthinking Cybersecurity: Performance Pitfalls for Autonomous Vehicles

Pete Herzog, *Co-Founder*
The Institute for Security and Open Methodologies

Security breaches don't happen because cybersecurity is hard; they happen because some people think it isn't. The concept of cybersecurity seems easy, and if you believe the compliance checklists, it really should be. Even the often-cited studies regarding what security professionals do for their personal security compared to those not in the field are woefully inadequate and misleading. Studies like those are good at making a point but are too narrow and incomplete to actually serve as valid instruction.

Even using strong passwords, which is one item on every security hygiene list, sounds like solid security advice. But for an organization, ensuring that principle is in practice is actually pretty complex. It impacts every single person in many authentication schemes, and has many moving parts from password managers to generating certificates and working with vendors.

In the end, the practice of making good passwords is far beyond the ability of most organizations to do more than just pass on this advice to employees. This is because many have IT staff tasked with security responsibilities but not much security experience.

Furthermore, we have come to rely on tools like "Top 20 Security Controls" that overly simplify the tasks required. It's like the difference between telling someone to build a rocket and actually being the person who has to build it; there are more actual steps to completing the task than it sounds like.

Yet, such lists are treated like NASA-approved rocket engineering schematics when they're nothing more than a collection of opinions about best practices that were determined by committee. The truth is that there's woefully too little scientific security research to back up those decisions, which is why we end up resorting to mere opinions. All of which brings us to the problem of why cybersecurity is hard.

SECTION 3

Security At The Speed Of Innovation

The key here is that you need to know more than your adversary about how something works and that it can go in two directions: deeper and broader. To know something more deeply isn't just about the way it's built, you need to get right down to the physics of it — even understanding the interaction of the particles of which it's made. The same is true for knowing something more broadly, where you understand the connectivity between things better whether or not they're in the same environment.

Our ability to see deeper and broader requires understanding events at the finest possible point of interaction. That's why as technology gets better, we can see things we couldn't previously. So, technology innovation moving quickly doesn't impact cybersecurity because there's always new things to secure in new ways. However, it does require a deeper and broader understanding of what we need to secure, which is hard to keep pace with.

A Risk In Time

In security, everything and everyone matters; security is about protecting it all. This is why risk analysis is poorly suited to the security of critical systems. In risk, there is always a loser, and sometimes the loser is you. Risk has you build your biggest protections around the most important systems and the systems most likely to be attacked.

However, the actual probability of knowing what system an attacker will choose to exploit cannot be known. The most important system to the infrastructure may not be the most important one to the attacker, because they are not interested in what the risk analysts think are important. That's the trouble with risk analysis: with limited resources you need to secure what you can to "keep going", which puts it at direct odds with customers because "keep going" is about the business and not about them.

Cybersecurity is about protection, and that means everything: the cars, the drivers, the owners, the buyers, the sellers and all the networked equipment in-between. Everything matters. Where the money can't be spent is not a consideration, because if it can't be secured then it can't be there. You can't have a service you can't protect, and if you do, that's taking a risk.

Ultimately, all risks are financial to the manufacturer. But to the consumers — those who are actually harmed when the risk doesn't go in the manufacturers favor — they're not just financial. So, there are no shortcuts to cybersecurity in critical systems. Everything and everyone matter. But in that light, it's ultimately people that make security difficult to sustain.

Securing Against Human Nature And The Skills-Shortage

From a security standpoint, people are chaotic, messy and sticky. They don't just *use things*; they rearrange them and personalize them, they leave messes behind and there's no way to know what they may do next — even if they're "security awareness" trained. Decades-old stories exist of people using the CD tray on their PC as a cup holder. Today they use the network as their personal leisure for downloading apps, bringing in their own gadgets to use, and even passing on their logins for friends and families to use. People are a vulnerability in systems.

Take a computer system and leave it in a default state with no user accounts, no personalization, or — in good English, *no nuthin'* — then try to break in and you'll find the attack surface is rather small. But give it to a person and in days they will more than triple the attack surface through personalization of that computer system. It's a commonly accepted concept in security that each interactive decision a person has with a system (like turn this on or off, install this, change this) is the risk equivalent to one vulnerability.

This problem is compounded in modern systems where the personalization leaks onto mobile phone apps, web application services for administration or support, and personalized services across networks, clouds, payment systems and countless third-party vendors for everything from helpdesk to software distribution platforms. That's when you begin to see a connected car isn't just an internet-enabled car; it's a system that is part of dozens of other systems with thousands of people in the sticky mix.

All of these systems require security analysis, trust analysis and privacy analysis, which doesn't seem out of the ordinary. However, every one of them requires the hiring of skilled people to do those tasks, which is something the world is in very short supply at this moment. Most major companies are desperate to fill their security personnel positions, with current estimates at about a 2.2-million-person deficit worldwide for cybersecurity. Which means, statistically, that some of those

companies' parts of the system are not going to have the people to adequately secure them or are going to have only unseasoned professionals to do so, which can be just as bad.

Therefore, makers of critical systems can't just assume their vendor will do their job when it comes to cybersecurity. They also can't just go with the lowest bidder which likely won't have the resources to assure they are adequately securing their end of the system. That means manufacturers of network-connected cars need to evaluate each vendor for trust and security as well as design protections from weaknesses, both in their vendors and their vendors' partners as well.

Why We Can't Just 'Fix The Bugs' To Make Autonomous Vehicles Secure

Testing the security of anything is hard and for a very good reason. Each single point of interaction with the thing, each knob you can turn, button you can push or query you can make requires 1,080 data points to be analyzed for security. This specific number was derived from research conducted by the *Institute for Security and Open Methodologies (ISECOM)*, which publishes the international security testing and analysis standard called *The Open Source Security Testing Methodology Manual*,[65] or *OSSTMM* (pronounced *aw-stem*).

According to the research, security requires the analysis of 12 controls (including authentication, indemnification, non-repudiation, etc.) for each of three operational parameters (accesses, trusts and visibilities) for each of six types of possible communication channels (data networks, wireless communications, etc.) and five different types of possible limitations (vulnerabilities, anomalies, etc.).

By analyzing one data point per second, it would take approximately 18 minutes of non-stop analysis for each and every interaction. Even simple systems have thousands of interactions or more, so you can see the exponential nature of the issue here. Consequently, more complicated systems like autonomous vehicles with hundreds of sensors and multiple user-interactive applications can easily have millions of interactions.

At 18 minutes per interaction, it will require more than 12,000 days to properly and thoroughly conduct security analysis. And that's just for the user interactions; this number doesn't take into consideration all of the interactions within software that could have bugs or operate incorrectly due to damage from heat, vibration or jarring — all things that happen to cars. Which means just by moving the car off the factory floor we could be creating new and possibly very specific vulnerabilities in the systems.

Testing the security of anything is hard, and for a very good reason. Each single point of interaction with the thing, each knob you can turn, button you can push, or query you can make requires 1,080 data points to be analyzed for security.

SECTION 3

Security Is More Than Patching Vulnerabilities

Unfortunately, what the typical person knows of security is usually limited to vulnerabilities and the patching of those vulnerabilities. To be honest, there's so much to do around "known" vulnerabilities alone that, despite having the assistance of automated scanners and automated patching, the work can be exhausting and yet still not exhaustive. Yet known vulnerabilities only make up a small part of security.

By "known" we mean vulnerabilities which have been publicly announced. The other part, the unseen part of the security iceberg, is comprised of all the vulnerabilities that have yet to be discovered. We also don't know if such vulnerabilities are only unknown to us, and we don't know what threats could exist tomorrow that can practically, efficiently, or persistently abuse those vulnerabilities. These are the vulnerabilities the scanners can't help with.

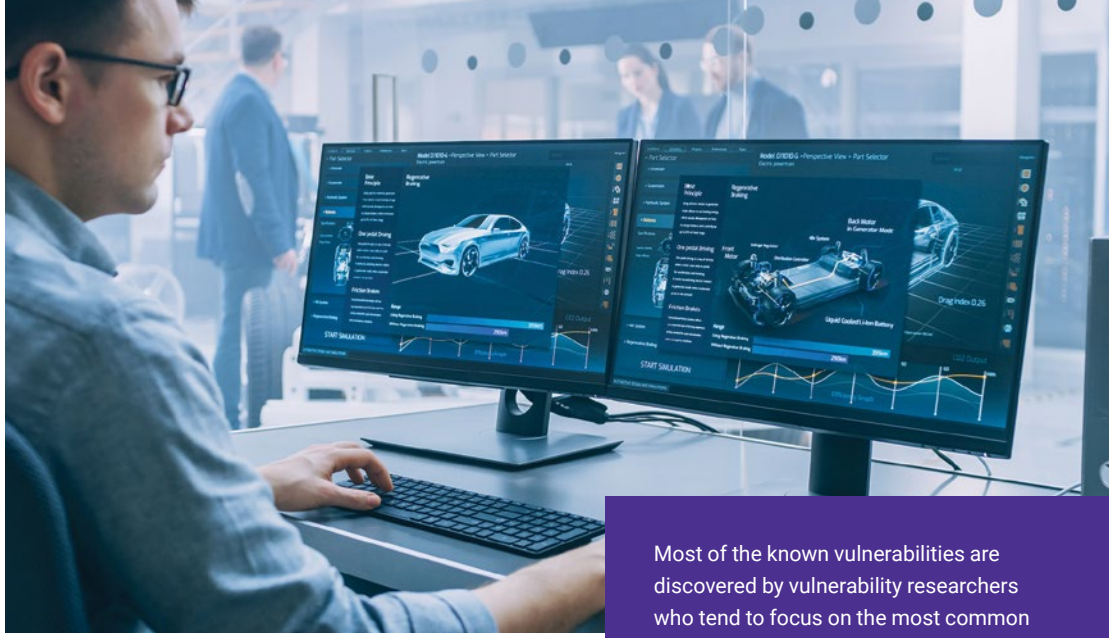
Most of the known vulnerabilities are discovered by vulnerability researchers who tend to focus on the most common software applications in order to either do the most good for the most people, or to get the biggest rewards for their discovery. This means niche software and third-party libraries, which even the popular software depends on to run correctly, may not receive equal vulnerability research time.

The fact that I had to rewrite that last sentence multiple times to state it factually should highlight that we honestly don't know, and while logically it is likely true, we have no empirical studies to corroborate this fact. Which brings us to the next problem, the lack of useful security research.

Not All Security Research Is Equal

Subject areas like vulnerabilities and risk tend to dominate the research field. Meanwhile, many other unexplored issues exist and lack meaningful studies. It is possible that in cases where a premise is surmised as "true" by the opinions of pundits, no reputable, empirical studies have been conducted to prove them out.

For example, we have no study that compares the losses caused by unmitigated vulnerabilities to that of the losses caused by poorly crafted patches that negatively impact operations. And while we'd like to err on the side of caution, this is truly an area where we don't know which outcome is worse when it comes to specialty software — especially software in critical systems, which may be a matter of life and death. At the end of the day, whether it's at the hands of a criminal hacker, due to a software bug or a poorly implemented patch, a fatality is still a fatality.



Most of the known vulnerabilities are discovered by vulnerability researchers who tend to focus on the most common software applications in order to either do the most good for the most people, or to get the biggest rewards for their discovery.

Therefore, especially for critical systems, we need to look far beyond patching vulnerabilities to include managing risk for all the unknown vulnerabilities which can be exploited by a malicious actor, as well as for any new software bugs created through normal operations. We need to proactively use operational controls to protect systems against threats which aren't known or don't exist yet — even for technologies that don't exist yet — which sounds like an impossible task, but it's not.

Security Testing By-The-Numbers

The method for thorough security testing and analysis is so straight-forward, it is almost a color-by-numbers kind of simple. We know that we can't secure something if we don't know how it works, yet it's more than that: we also can't secure something if we don't understand the mechanics of the environment it is intended to operate in, or how it communicates and interacts with users and other systems, or all the resources it requires in both the physical and cyber-worlds.

This is the basis for what is known as the Four Point Process, or 4PP for short, as outlined in the OSSTMM. The 4PP is how we can effectively analyze, test and build-in security for anything, and it's based on the fact that all security is about interactions. There are four main areas of interactions, which I'll try to explain here without using the overly technical OSSTMM terms for them:

- **Interactions:** You throw something at me, and I throw it back — that's an interaction. You ask me a question and I answer: an interaction. You make a loud noise near me, and I react, etc. Interactions are combinations of actions and the corresponding reactions.
- **Emanations:** You observe a thing and it smells funny, or it flashes a light, or it makes a sound, or an electromagnetic wave in the 2.4 GHz frequency range, or a strange vibration is coming off of it accompanied by five volts of electricity. These are emanations, the things it gives off. Sometimes that emanation tells you something about the thing and sometimes it doesn't.
- **Environment:** The place where the thing resides is its environment — cars have streets, applications have an operating system, servers have a network, etc. The environment does two things: it frames what the thing can do while in the environment, and it frames what anyone can do trying to get to that thing in that environment. Understanding the details lets us understand the environment.
- **Resources:** The things that a subject needs to keep going — for an application it could be certain software libraries or even specific variables or formats of those variables; it could be climate control, power, vibration control or even suitably licensed drivers. The required resources show the limits of what the subject can do during a specific time period. Changes in resources lead to changes in the subject's outcomes.

The 4PP are what you need to understand to secure something effectively. Actually, it's everything you need to know. Working from the 4PP as a foundation, an effective security plan for connected and autonomous vehicles will look something like this:

- Security testing and analysis of infrastructure components including servers, networking equipment like routers and switches, and applications on web and mobile devices including analysis of the functions of resilience, continuity and non-repudiation in the system.
- Security testing and analysis of user-interactive security systems including authentication, confidentiality and privacy. Security and trust analysis of supply chains including helpdesk, development, IT, network, management, system, and user administration and vulnerability management.
- Security testing and analysis of security equipment for proper configuration and functionality including firewalls, web application firewalls, SIEM, antivirus and any other security mechanisms in use.
- Security testing and analysis of the automobile's connected components, a gap analysis of security controls for all interactive points in the system and the car and more…

Conclusion

The real cat-and-mouse game with security testing ultimately comes down to who can make the better tools in order to see the most details at the macro and micro levels in whatever is being tested — us or our adversaries. That's it. Anything less is would be an acceptance of the fact that the product is going to market with exploitable vulnerabilities.

While the concept of security is simple, the process is hard. There is no shortcut for effective security, but achieving a state of effective security testing for the development of safe autonomous vehicles is objectively possible if we are willing to commit the resources necessary.

Pablo Picasso famously stated that it took him just four years to learn how to paint like the Italian renaissance master Raphael, but despite all his skill and his mastery of technique, it took him a lifetime to learn how to paint like a child. Sometimes simple is so hard.

Pete Herzog is the Co-Founder of the Institute for Security and Open Methodologies (ISECOM). He created the OSSTMM, the international standard on security testing and analysis and its Cybersecurity Playbook. He also founded Hacker Highschool, which teaches cybersecurity awareness for teens.

SECTION 3

Connected and Autonomous Vehicles: Policy, Performance and Peace of Mind

Parham Eftekhari, *Executive Director*
Drew Spaniel, *Lead Researcher*
ICIT

In the 1950s and 1960s, vehicles were not developed with seat belts, crumple zones or other safety features because automobile manufacturers prioritized aesthetics and costs over safety. This did not change until the legislative community intervened, driven by consumer advocacy and influential policymakers like Ralph Nader. These groups sought to mandate safety controls in the form of automobile safety regulations.

Without meaningful regulatory oversight, autonomous vehicles risk being similarly developed without security controls sufficient to protect consumers from life-threatening risks. The current culture around software development often uses consumers as crash test dummies of sorts for potentially vulnerable applications with inadequately screened code.

Most consumers lack the capacity to evaluate the security of the products that they purchase. Therefore, there is little external pressure for technology manufacturers to ensure that they develop products with layered security controls throughout the software development lifecycle.

Responsible regulatory legislation is one tool that the transportation sector can use to ensure the safety of autonomous vehicles, although it will be a difficult goal to achieve. One of the challenges in developing regulatory legislation and frameworks that rely on non-compliance penalties is that they often fail to encompass the scope of the risk regarding insecure software. This is because policymakers may lack a comprehensive understanding of cybersecurity best practices and the underlying technology being regulated.

Additionally, autonomous vehicle manufacturers will likely exert their influence on policymakers to deter or alleviate regulatory frameworks that they believe will stifle innovation. Meanwhile, consumers who typically focus on the promise of

SECTION 3

convenience and features will be distracted by the obfuscation of privacy and security risks that come from a combination of a lack of awareness and legacy industry practices.

Overcoming these challenges requires education and engagement of consumers, policymakers and the autonomous vehicle industry. Automobile manufacturers must recognize that including security at each stage of the lifecycle will not inhibit innovation or decrease profits. Instead, it will enable more rapid adoption of new technologies. Policymakers should learn enough technical nuances to enact legislation that will incentivize manufacturers to build security into the product lifecycle. Consumers must be educated on security and privacy risks while being reminded of the power that they can exert over the market. This comes in the form of buyers who demand safety and security as priority features.

While much work must be done, the National Highway Traffic and Safety Administration (NHTSA) framework and the proposed *S. 2182: The SPY Car Act* represent two strong steppingstones. Together, they accomplish some of these goals and steer the autonomous vehicle industry toward a more robust and resilient future.

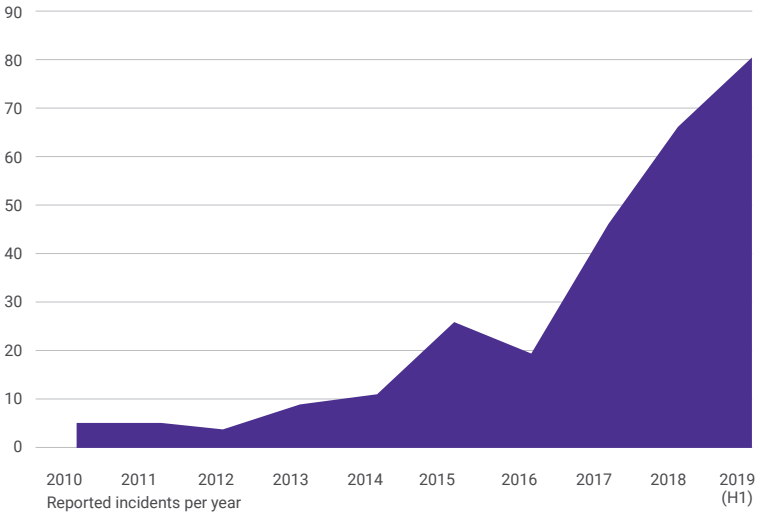
The Threat Landscape Surrounding Autonomous Vehicles Is Expanding

The number of reported cyberattacks targeting connected devices in 2018 was more than six-times those reported in 2015. One repository of data tracking cyber incidents involving the Smart Mobility ecosystem cites 311 cases since 2010, with a drastic spike in more recent years.

Targets for adversarial campaigns include vehicle onboard computers, connected alarm systems, infotainment units, telematics, ECU vulnerabilities and more. Essentially, if it is connected to a smart car and it controls a system or collects data, then an adversary of one category or another will be interested in targeting it. For instance, a nation-state actor might attack a GPS system to cause chaos within major cities if the autonomous vehicles that depend on guidance from that GPS network lack redundant navigation subsystems. Similarly, a cybercriminal could poison an update server with ransomware and demand payment from the manufacturer once individual vehicles are infected. Even an unexploited vulnerability left in the hundreds-of-millions of lines of code underlying autonomous vehicles subsystems could cause a catastrophic incident if that portion of poorly developed code does not interact with other systems as intended.

> **Essentially, if it is connected to a smart car and it controls a system or collects data, then an adversary of one category or another will be interested in targeting it.**

Rapid Growth in Cyber-Attacks on Smart Mobility 2010–2019



Source: Upstream Security Global Automotive Cybersecurity Report 2019

Securing Autonomous Vehicles Requires Meaningful Regulation

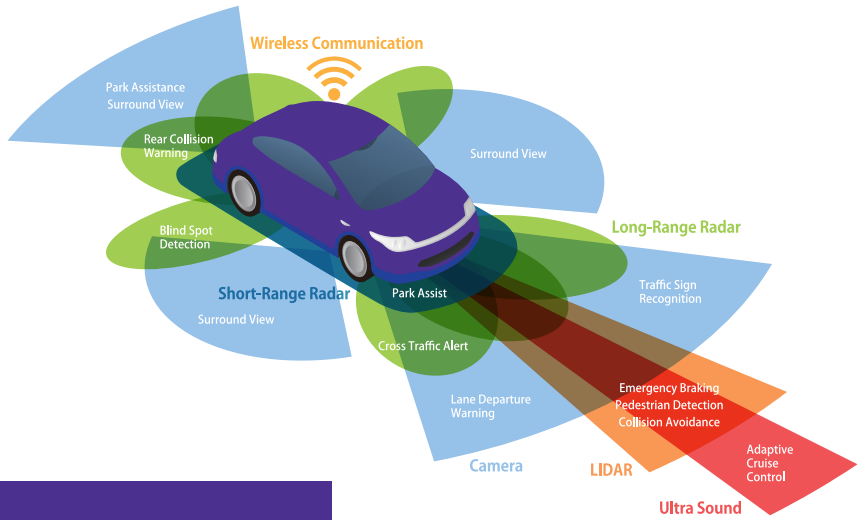
Ensuring a sustainable autonomous vehicle ecosystem requires policymakers to understand the need for comprehensive cybersecurity controls. It also requires them to write responsible, meaningful legislation that will protect consumers by mandating auto-manufacturer security while ensuring regulations don't disincentivize innovation. Some areas of focus for meaningful autonomous vehicle cybersecurity guidance and regulation include:

- Supply chain security
- Secure coding practices
- Security-by-design throughout development

SECTION 3

- Layered security throughout the hardware and software stack
- Threat intelligence sharing
- Consumer privacy protections
- System reliability and autonomy controls
- Manufacturer accountability
- Secure update procedures
- Penetration testing to reduce zero-day vulnerabilities
- Ensuring that boards include a C-level cybersecurity position and a CISO to oversee the business unit
- Comply with NIST and other best practice frameworks

Currently, a number of legislative initiatives are ongoing within the House and Senate regarding autonomous vehicles, artificial intelligence and cybersecurity. However, only one piece of legislation introduced in 2019 addresses all three topics: *S. 2182: the "Security and Privacy in Your Car Act of 2019"* also referred to as the *"SPY Car Act of 2019."*



Every subsystem, sensor, protocol and data repository that autonomous vehicles depend upon is at risk of adversarial campaigns.

Image Source: MachineDesign

The SPY Car Act of 2019

S. 2182 was introduced on July 18, 2019, by Senators Ed Markey [D-MA] and Richard Blumenthal [D-CT]. It amends *Chapter 301 of title 49, United States Code* to include cybersecurity standards in relation to autonomous vehicles. It sets specific definitions of critical system software, driving data, data access/entry points and hacking. More importantly, it sets cybersecurity standards for all vehicles manufactured for sale in the United States within two years of the inaction of the Act.

> **One common struggle facing the regulation of the majority of technology fields is the juxtaposition of the break-neck pace of technology contrasted against the grueling drudge of regulatory bureaucracy.**

The Act requires that "all entry points to the electronic systems of each motor vehicle manufactured for sale in the United States shall be equipped with reasonable measures to protect against hacking attacks." It mandates that critical software systems be isolated from non-critical systems. In addition, it requires all systems be "evaluated for security vulnerabilities following best security practices, including appropriate applications of techniques such as penetration testing." The Act also directs auto manufacturers to reasonably secure all electronic systems that are built into motor vehicles that collect driving data as to prevent unauthorized access or disclosure of the information under three conditions: 1) while the data is stored onboard the vehicle, 2) while the data is in transit from the vehicle to another location and 3) in any subsequent offboard storage or use of the data.

Finally, the Act requires that "any motor vehicle manufactured for sale in the United States that presents an entry point shall be equipped with capabilities to immediately detect, report, and stop attempts to intercept driving data or control the vehicle."

One common struggle facing the regulation of the majority of technology fields is the juxtaposition of the break-neck pace of technology contrasted against the grueling drudge of regulatory bureaucracy. Often, by the time meaningful legislation passes the House, Senate and Executive Branch it is already outdated in some way. Either the purpose of the technology has shifted or new capabilities have introduced additional regulatory challenges. The *SPY Car Act of 2019* addresses

this potential obstacle by including a timeline that accounts for regular updates and adjustments in the measures. Within 18 months of the enactment of the bill, the Administrator of the National Highway Traffic Safety Administration, after consultation with the Federal Trade Commission, will issue a notice of proposed rulemaking to carry out section *30129 of title 49, United States Code*, and they will promulgate final regulations within three years. Every three years thereafter, the Administrator, in consultation with the FTC, will review the final regulations and update them as necessary.

Cybersecurity As Part Of A Consumer Decision-Making Process

As mentioned in ICIT Fellow Malcolm Harkins' essay *The Rise of the Cyber Industrial Complex and Expense in Depth*,[66] consumers are not informed parties regarding the cybersecurity of the technology that they purchase. As a result, there is little incentive for companies to include comprehensive cybersecurity controls throughout the system and there are few, if any, consequences for companies that release vulnerable products.

Though some regulatory frameworks lean on penalties and fines to disincentivize the release of insecure products, the scale of the fine is often wildly insufficient to incite proactive security efforts. Without additional pressure, for a company generating billions in profit, the rational economic decision is for a company to release insecure products and incur a few million in fines or lawsuits. The benefits outweigh the consequences by at least an order of magnitude.

> **… cybersecurity needs to be one of the pillars of the acquisition process alongside cost, schedule, and performance.**

Only through market pressure that threatens the bottom line can consumers compel manufacturers to include layered security at each stage of the development lifecycle. As discussed in ICIT's publication, *Software Security is National Security*,[67] cybersecurity needs to be one of the pillars of the acquisition process alongside cost, schedule and performance.

S. 2182 introduces cybersecurity considerations into the consumer purchasing decision by requiring that each vehicle manufactured for sale in the United States to display a cyber dashboard label that informs consumers "through easy to understand, standardized graphic about the extent that the motor vehicle protects the cybersecurity and privacy of motor vehicle owners, lessees, drivers, and passengers beyond the minimum requirements under section *30129* of this title and in *section 27* of the *Federal Trade Commission Act*."

Privacy Safeguards

S. 2182 requires vehicle manufacturers to provide each owner/lessee a clear and conspicuous, plain-language notice of any collection, transmission, retention or use of driving data collected by the vehicle. Consumers are then provided the option to opt-out of any collection or retention of driving data without the risk of losing access to navigational tools, or other features or capabilities within technical possibilities.

Data required for post-incident investigations emissions history checks, crash avoidance or mitigation and other regulatory compliance programs are exempt from consumer opt-out. Without affirmative, express consent, manufacturers or associated third parties may not use collected vehicle information for advertising or marketing.

NHTSA Is Working To Proactively Ensure Vehicle Cybersecurity

Autonomous vehicles could increase the efficiency and capacity of human transportation, so it is paramount that as technology develops, security is a defining parameter. As one of the primary regulators of autonomous vehicles, it is the responsibility of the NHTSA to ensure these technologies are deployed safely, expeditiously and effectively. The organization also sees that they take steps to mitigate emerging challenges, including cybersecurity. NHTSA has developed a multilayered cybersecurity framework that leverages the *National Institute of Standards and Technology Cybersecurity Framework* and encourages industry to adopt practices that improve the cybersecurity posture of their vehicles in the United States.

NHTSA's goal is to collaborate with the automotive industry to proactively address vehicle cybersecurity challenges and to continuously seek methods to mitigate associated safety risks. The guidance focuses on a vehicle's wired and wireless entry points, and the layered approach reduces the potential for an adversary to exploit a vulnerability, reduces the possibility of a successful vehicle cyber-attack and mitigates the potential consequences of a successful intrusion. It states that the comprehensive and systematic approach to developing layered cybersecurity protections for vehicles includes the following:

SECTION 3

- A risk-based prioritized identification and protection process for safety-critical vehicle control systems;
- Timely detection and rapid response to potential vehicle cybersecurity incidents on America's roads;
- Architectures, methods and measures that design-in cyber resiliency and facilitate rapid recovery from incidents when they occur; and
- Methods for effective intelligence and information sharing across the industry to facilitate quick adoption of industry-wide lessons learned.

NHTSA encouraged the formation of Auto-ISAC, an industry environment emphasizing cybersecurity awareness and collaboration across the automotive industry. NHTSA's current research into improving vehicle cybersecurity includes:

- Anomaly-based intrusion detection systems research: Researching metrics and objective test methods to assess the effectiveness of such solutions.
- Cybersecurity of firmware updates: Researching cybersecurity of automotive electronics update mechanisms through physical and over-the-air means.
- Cybersecurity considerations for heavy vehicles: Researching similarities and differences between passenger cars and larger vehicles from a cybersecurity considerations standpoint.
- Research on reference parser development for V2V communication interfaces: Developing a formally verified and mathematically proven message parser for V2V communication interfaces.
- In-house cybersecurity research at the Vehicle Research and Test Center (VRTC) in East Liberty, Ohio: This research explores the cybersecurity risks of today's vehicle electronic architectures. It aims to establish principles and guidance that could improve the cybersecurity posture of passenger vehicles through applied research.

NHTSA regularly collaborates with other government agencies, vehicle manufacturers, suppliers and the public to further industry's efforts in addressing vehicle cybersecurity challenges. The objective of this strategy is to promote the impact of the various safety applications employed in current vehicles, as well as those envisioned for future vehicles that may feature more advanced forms of automation and connectivity.

NHTSA's approach to vehicle cybersecurity has the following goals:

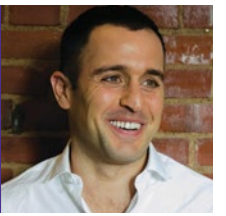
- Expand and share the automotive cybersecurity knowledge base to better establish comprehensive research plans and develop enabling tools for applied research in this area;
- Support the automotive industry in implementing effective, industry-based best practices and voluntary standards for cybersecurity and participate in cybersecurity information-sharing forums;
- Foster the development of new system solutions for automotive cybersecurity; and
- Determine the feasibility of developing performance evaluation methods for automotive cybersecurity.

Conclusion

It is important to empower consumers to care about autonomous vehicle cybersecurity and to incentivize manufacturers to develop secure systems through meaningful, responsible legislation. ICIT believes that S. 2182 demonstrates that Congress is paying attention to autonomous vehicle cybersecurity and that the NHTSA framework highlights the collaborative approach that government regulators are adopting to encourage security-by-design in the autonomous vehicle development community.

While perhaps imperfect, they represent formidable starting points for the industry and are the types of efforts needed to improve the resiliency of this segment of the transportation sector.

Parham Eftekhari is the Founder and Executive Director of the Institute for Critical Infrastructure Technology (ICIT), the nation's leading cybersecurity Think Tank. The group provides objective, non-partisan research and education to public, private and legislative stakeholders.



Drew Spaniel is the Principal Research Analyst in cybersecurity, technology and data science at ICIT. He also looks at emerging adversarial trends, threat actor profiling, and legislation and agency initiatives related to information security and privacy.

SECTION 3

Forging the Path for Automotive Safety Standardization

Chris Hobbs, *QNX Software Systems Safety Specialist*
BlackBerry QNX

Engineers working on the design of safety-critical embedded systems are at a nexus of storms blowing from several directions. The whole concept on which safety analysis has been based for many years has been found inappropriate for today's systems; we have no coherent mechanism for handling an increasingly important element of safety; a component of our systems that we have typically ignored is becoming dominant; our traditional method of system verification is becoming ineffective; and we are developing systems in a way that prevents us from understanding their behaviour.

This article considers these winds of change and, based on decades of safety and security experience, offers the beginnings of a possible path forward.

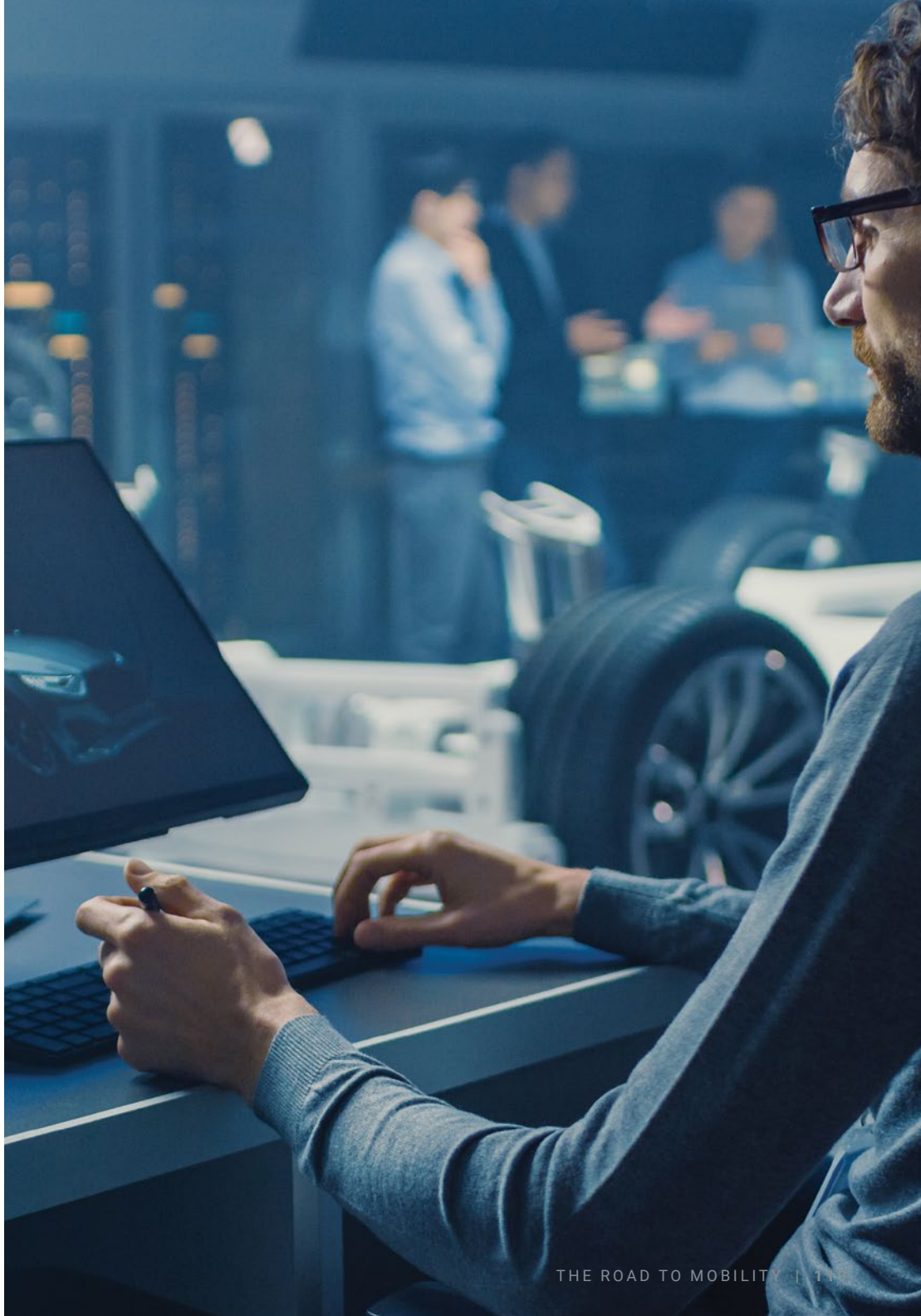
Failure And SOTIF

Traditionally, analysis of the safety of systems has been an analysis of failures. It was assumed that a system became dangerous only when one of its components malfunctioned. This approach is reflected in IEC 61508, which categorizes systems according to the probability of dangerous failure per hour of use (for example, 10−7 for Safety Integrity Level 3). It is also explicit in ISO 26262 (second edition), which defines a "hazard" to be a "potential source of harm caused by *malfunctioning behaviour* of the item" (my emphasis).

Many papers and books by Nancy Leveson and her team build on the work of Jens Rasmussen when pointing out that many, if not most, dangerous situations do not occur as the result of a component failing.[68]

The following observes the landscape as it appeared in 2004:

> *Accidents resulting from dysfunctional interactions among system components… have received less attention than component failure accidents. This lack of concern may stem partly from the fact that in the simpler systems of the past, analysis and testing allowed exercising the system to detect all potential undesired interactions and changing*



the system design to eliminate them. Increasing complexity and the introduction of software control is reducing this ability and increasing the incidence of system accidents.[69]

This article describes a batch chemical reactor in England that discharged its contents into the atmosphere as a result of an incident in which every component behaved exactly as it was intended: nothing malfunctioned. But, by coincidence, a catalyst was introduced into the reactor at the same time that an alarm detected in another part of the system.

This behavior can particularly be expected from "accidental systems," and it was recognized as early as 2003 that machine learning leads to such systems.[70]

The behavior of many systems, including (semi-)autonomous road vehicles, autonomous ships,[71] drones, medical devices and vacuum cleaners, is based on learned information. For such systems, it is accepted that the traditional failure-based approach is inadequate. The term "SOTIF" (Safety Of The Intended Functionality) has been coined for the new form of analysis.

Software, Hardware And Data

Machine learning presents a new challenge to safety analysis because it puts the emphasis neither on software (which in an artificial neural network is trivial) nor hardware, but on data. IEC 61508 and ISO 26262 have separate sections on hardware and software considerations but cover data only in passing.

Since 2014 the Data Safety Initiative Working Group (DSIWG) of the Safety Critical Systems Club has been working on guidelines covering the consideration of data in a safety analysis. The group issued version 3.1 of this guidance in February 2019. Appendix H lists some 27 incidents where data errors, rather than hardware or software failure, caused dangerous situations. It is hoped that the guidelines produced by the DSIWG will be incorporated into the relevant international standards as those standards are updated.

Data And Machine Learning

One area where data are particularly important is that of systems built through machine learning. With the exception of a few hundred lines of software, the behaviour of an artificial neural network or support vector machine is determined exclusively by the learned "weights".

Classical analysis considers the integrity of these weights, given the possibility of corruption through memory bit-flips,[72] row-hammering[73] and other forms of cross-talk and electro-magnetic interference.

Even this is a challenge in an environment where there are many weights—as is typical for a deep neural network—because it significantly slows down the algorithm if the correctness of every value accessed from memory is checked. Car manufacturers are already facing challenges in the amounts of memory and processing power required to make a forward pass through the neural network.

However, there is a deeper challenge — that of the intended functionality. The major question here is, "What do the weights actually represent? What has the machine learned?"

There are numerous examples of apparently well-trained networks failing when presented with a new environment because they have learned irrelevant details. One well-known example concerns a military system taught to distinguish between pictures of woodland containing tanks and pictures of woodland without tanks. Such an automated system would reduce the human workload in scanning photographs for tanks. The system learned to be almost 100% accurate on the hundreds of photographs on which it had been trained but was no better than random on new photographs. On investigation, it was found that most of the training photographs that contained tanks had an overcast sky, whereas most of the photographs without tanks had a blue sky. The network had merely learned to distinguish between cloudy and clear skies.

During my lifetime, I estimate that I have driven a car for about 20,000 hours. In all that time I have never had a man dressed in a chicken suit cross the road in front of me. However, if I meet such a situation when driving home from work this evening, I shall probably be able to cope.

What about an autonomous car? Its camera system would perhaps detect a chicken, but its "reasonableness" filter might reject that, because chickens are not 1.9 meters tall. Similarly, there are reports of such systems rejecting children on skateboards because, although the image looks like a child, it is moving at a speed much faster than a child could move.

Pavement Patty, bouncing her ball across the road in Vancouver, has attracted a lot of attention. She does not exist, being just a picture drawn on the road, but she could certainly confuse an autonomous car: the camera indicates that a girl is present; the LiDAR indicates that there is nothing there.

It is argued that the probability distribution of such edge cases as men in chicken suits and pictures of girls painted on roads is heavy-tailed and this presents a serious problem.[74] There will be many of these types of events, but it is not useful to train cars to react correctly to them because they will almost certainly never meet any particular event during their lifetime.

SECTION 3

UL 4600 ("Standard for Safety for the Evaluation of Autonomous Products") is due to appear in late 2019 and proposes a safety case approach to demonstrating that an autonomous car is sufficiently safe. This is a goal-based (rather than prescriptive) standard but is specific for automobiles.

Harvard law professor Jonathan Zittrain points out that we have often deployed solutions that work, even if we don't have an underlying theory for how they work.[75] For example, aspirin has been used since 1897 to reduce pain, but it was only in 1995 that we understood how it works. Zittrain makes a powerful argument that doing so involves us in "intellectual debt". Until we understood how aspirin worked, it was difficult to predict how it would interact with other drugs.

Similarly, it is difficult to predict how a learned network that we do not understand will interact with other networks when it is incorporated into a larger device.

Safety And Security

It the distant past, many embedded, safety-critical systems were secured by physical security. The device was locked in the cab of a train or kept in a locked and protected area of a shop floor. These devices were largely self-contained and had few external interfaces.

Today there are few such devices. Almost every one has Wi-Fi and Bluetooth connections and relies on GNSS (e.g., GPS or Glonass) for its operation. All of these can easily and cheaply be blocked or spoofed by an attacker. Once access is gained, vulnerabilities in the processor hardware (Meltdown, Spectre, Spoiler, Management Engine, etc.) and memory[76] can be used to subvert the device's behavior, making it unsafe.

Machine learning can also provide opportunities for hackers to make a device act dangerously. Devices that continue to learn once they have left the factory are particularly vulnerable to malicious people deliberately training the system to do dangerous things. For car systems, these unsafe learned practices could then be disseminated to other cars from the same manufacturer.

Various studies[77] have been carried out to find how neural networks can be reverse-engineered so their weak areas can be identified and attacked. This has been particularly successful with corrupting pixels on camera images in cars: A neural network can take two images that appear to be identical to a human viewer and "notice" a human crossing the road in one version, but completely miss that human in the other.

Security and safety are inter-related and antagonistic (Increasing one decreases the other. For example, consider locking the door of a theater.) and so cannot be considered separately. However, there are no clear guidelines on how to balance them in embedded systems. ISO/SAE 21434 is in preparation, but focuses on security in road vehicles, not all embedded systems.

Pavement Patty, bouncing her ball across the road in Vancouver, has attracted a lot of attention. She does not exist, being a picture drawn on the road, but she could confuse an autonomous car, the camera identifying the girl, the LiDAR indicating that there is nothing there.

Verification

Dynamic testing has been used for many years as a means of verifying the correct operation of a system. It is a process whereby a finite set of particular situations is presented to a system and its behavior is observed. Unfortunately, this idea has become largely ineffective for several reasons:

- No finite collection of situations can come close to exploring the state space of a modern system.
- A test detects failures, but only faults can be fixed. In many cases, particularly with Heisenbugs, tracing the failure back to the fault is very difficult or impossible.
- Even if the fault can be found and corrected, recreating the circumstances that created the failure (to check that the fix is correct) is likely to be impossible. Perhaps it requires an interrupt of type X to occur within 2.3µs of thread T_1 attempting to lock mutex M1 when that mutex is already locked by thread T_2, which has had its priority increased to 23 by virtue of contention for mutex M_2 with thread T_3 . . . . It would be impossible to reproduce that precise situation.

The recognition of these weaknesses is not new. A 1976 article in *IEEE* says:

> *. . . [imagine] a 50 line program consisting of 23 consecutive "IF THEN" constructs. Such a program could have as many as 33.5 million distinct control paths, only a small percentage of which would probably ever be tested. Many such examples of live Fortran programs that are physically small but untestable have been identified and analyzed by the tools described in this paper.*[78]

The software testing standard, ISO/IEC/IEEE 29119, also acknowledges these weaknesses: "*Dynamic testing is necessary, but not sufficient to provide reasonable assurance that software will perform as intended.*" ISO 29119 proposes a risk-based model for testing as one of a number of verification techniques.

As testing becomes increasingly ineffective, formal methods are becoming more powerful, yet they are fragmented and unstandardized.

SOTIF And STAMP

ISO/PAS 21448,[79] published in early 2019, is titled "Road vehicles — Safety of the intended functionality." Its approach is to divide potential road scenarios (e.g., the man in the chicken suit crossing the road ahead of the car) into four groups:

- **Area 1:** known (or expected) situations that are safe.
- **Area 2:** known (or expected) situations that are unsafe.
- **Area 3:** unknown situations that are unsafe.
- **Area 4:** unknown situations that are safe.

Area 2 is the area where traditional risk mitigation techniques can be applied, and this area is not considered further in ISO/PAS 21448. ISO 26262 covers this area for road vehicles and IEC 61508 for industrial applications.

The steps proposed in ISO/PAS 21448 also ignore area 4 and concentrates on converting scenarios in area 3 into area 1.

However, if heavy-tail distribution[80] is found to apply, it will militate against this approach.

ISO/PAS 21448 makes a passing reference to the Systems-Theoretic Accident Model and Processes (STAMP) model developed by Nancy Leveson and her group[81] but does not make use of the system-level concepts included in it. Research has also explored whether STAMP can be applied to an autonomous, automatic braking system in a car.[82]

I believe that an opportunity has been missed by restricting the specification to what is probably one of the most difficult of the autonomy problems: that of road vehicles. The marine industry is experimenting with autonomous container ships and ferries, and autonomous, machine-learning systems have been used for medical image scanning for many years. These may be simpler problems to tackle.

Mind The Gap!

There are several distinct strands in play at the moment:

1 Systems are becoming increasingly autonomous and will therefore meet unique and unusual conditions that they have not been explicitly programmed to handle.

2 Machine learning is being increasingly used to replace manually designed systems. Andrej Karpathy of Tesla has said that "*Software 2.0 is written in neural network weights. No human is involved in writing this code …*"[83] This may be deliberate hyperbole, but if this prediction is even largely true, then in a few years there will only be hardware and data. Software will have disappeared.

3 Security can no longer be ignored for safety-critical systems and there are no published standards on how to build a secure system. ISO/SAE 21434 is to appear as a Draft International Standard (DIS) in late 2019 or early 2020.

4 The software testing standard, ISO/IEC/IEEE 29119, explicitly recognizes that testing is an insufficient means of verification for any system, and this is particularly true of safety-critical systems.

5 A new version of ISO 26262 has been issued that specifically excludes any aspect of autonomy or machine learning. It still defines a hazard in terms of malfunctioning components and it only treats data and security en passant.

The Claims

The introduction to this article made some claims. We can now identify the factors behind those claims:

- Claim: "The whole concept on which safety analysis has been based for many years has been found inappropriate for today's systems." Failure analysis.
- Claim: "We have no coherent mechanism for handling an increasingly important element of safety." Security.
- Claim: "A component of our systems that we have typically ignored is becoming dominant." Data.

- Claim: "Our traditional method of system verification is becoming ineffective." Testing.
- Claim: "We are developing systems in a way that prevents us from understanding their behavior." Machine learning.

Research is being carried out to improve some of these weaknesses (e.g., building Selective Bayesian Forest Classifiers rather than neural networks so that the learned behaviour can be understood[84]), but these are point solutions to particular problems.

The Role Of Standards

We have a network of standards and specifications that leave serious gaps in the above areas.

The standardization process through ISO, IEC, UL, Cenelec and other bodies has historically focused on specialized areas. This can be compared to the model of safety analysis that Nancy Leveson presented in her work.[85] With today's systems of systems and accidental systems, it is no longer possible to analyze the safety of a system by considering its components individually. In the same way, I feel that it is no longer possible to standardize an approach to safety that has different working groups considering individual components of a modern system. We have to have apply a systems-wide approach not only to our safety analysis, but also to our standardization process.

In many areas, prescriptive standards are essential. It is good to know that if I buy an electrical appliance at a local shop, its plug will fit into the socket in my house. Indeed, it would be good if electrical outlets were identical around the world.

In other areas, prescriptive standards are, by their nature, out of date before they are replaced: locking in software techniques that have been superseded. Annex C of part 7 of IEC 61508 (second edition) lists references to papers describing techniques recommended elsewhere in the standard. Forty-five percent of these are from the 20th century and 21 percent of them predate 1990. It is also interesting that part 7 recommends particular programming languages for use in safety-critical systems. FORTRAN 77 and PASCAL are recommended or highly-recommended at different safety integrity levels.

A Way Forward?

Goal-based standards define the target to be met, rather than prescribing the steps that must be taken to reach it. The Safety Case then becomes the argument that the target has been reached. I believe that the combination of system-level, goal-based standards, together with a strong constraint on the associated Safety Case, is the only way to bridge the gaps listed above.

In some areas, prescriptive standards will still be required. For example, it is essential that the radio frequencies and message formats used for vehicle-to-vehicle communications be prescribed so that all cars can communicate with each other. However, in general, a systems approach to standardization implies a move towards goal-based standards. In particular, a goal-based approach is probably the only way in which the different demands of security and safety can be met.

The goal-based approach of UL 4600 is a significant step in the right direction, and I believe that the technique of using the Safety Case as the basis for safety claims is a sound one. BlackBerry/QNX is working with the Assurance Case Working Group of the Safety Critical Systems Club to bring its positive experience of using Eliminative Argumentation in Safety Cases to the relevant standards.[86]

At its meeting in Sydney in March 2019, the IEC's Market Strategy Board considered a white paper titled *Safety in The Future — Collaborative Safety: Beyond Mechanical and Functional Aspects*. That this type of whitepaper is being considered is a positive sign that there is recognition that system-level thinking is required. However, the standards bodies are large super-tankers that will require significant effort to deflect from their present course.

The danger in this approach can be summarized by the old saying: *"We had ten standards in this area, so we wrote another one to combine them. We now have eleven standards."*

Christopher Hobbs is a BlackBerry QNX Software Systems Safety Specialist working on the QNX kernel software. He has a particular emphasis on safety critical systems (IEC 61508, IEC 62304/ISO 14971, ISO 26262, EN 5012x)

SECTION 3

The Impact of Culture on Connected and Autonomous Vehicles

Kai Roer, *Co-Founder and CEO*
CLTRe (recently acquired by KnowBe4)

The innovations in the development of today's connected vehicles lay the groundwork to future autonomous vehicles. With this, a myriad of factors need to be considered in architecting automated decisioning engines with capabilities rooted in artificial intelligence and machine learning.

Some of the most apparent factors in the mix are around security of the systems involved and the potential impact the integrity of those systems can have on overall vehicle safety. What may not be as readily apparent is the influence the concept of culture has on both the approach to the development of those decisioning engines and the approach to securing them.

At the core of both initiatives will be outcomes based on determinations that will have far-reaching and long-standing implications on connected and autonomous vehicle technology. Additional considerations include how these technologies will effectively assimilate in our global society.

Those determinations will be firmly rooted in, and defined by, the concept of culture — more specifically by the array of perceptions that make up the notion of culture. This article lays the groundwork for considering the concepts that drive our understanding of culture and how integral it is in shaping the direction autonomous vehicle technologies will take.

Complexity And Nuance In Decisioning

Consider the following: a car is driving down the street, and in the car are two people conversing on a topic of no importance to this story. Neither person pays careful attention to the road and the traffic; they are instead deeply focused on themselves.

SECTION 3

Somewhere nearby, a group of kids are playing soccer in a garden; they laugh, they run, they kick the ball and play as children do. They are fully emerged in the game and paying no attention to their surroundings.

At the same time, an elderly person is slowly walking down the sidewalk approaching a crosswalk, proceeding to cross the street seemingly oblivious to their surroundings. As the elderly person is crossing, the soccer ball comes flying across the street in the opposite direction followed by one of the children who is running as quickly as they can and is looking only at the ball.

Down the street, the car with the conversing passengers is fast approaching on a direct collision course of the child — unless the driver changes the car's direction. If they do, they will instead strike the elderly person. A third option presents itself; the car may turn the other way and hit a trailer instead, but that will most likely kill both the passengers.

Now, you get to choose which of the three outcomes is the right one. What do you choose? Can we all agree what the right choice is? As it turns out, we cannot.

When we are deliberating what the "right" choice is before the fact, all kinds of moral, ethical and cultural dilemmas make our choice nearly impossible to make. It is, as it turns out, much easier to make this choice *after the fact* (if the driver were to be a human and not a computer, that is).

As humans, we accept a certain level of fallibility from each other. We also, then, accept that with difficult choices in some instances comes the potential for horrendous results. If you were driving the car in the above example and ended up killing someone, you would rationalize the choice you made in the context of all of the stakeholders.

People would still get harmed by your choice, but as a society, we have a certain set of rules and explanations that help you and others to understand and accept the particular choice that was made. These rules and explanations are considered part of culture, defined as the *ideas, customs and social behaviors of a group [of people]*.

In developing autonomous systems, we have a certain expectation that these systems should behave with a high level of perfection in every choice they make. Programmatically, that is not that hard to accomplish if we simplify all things dramatically and keep the number of possible choices extremely limited. In a lab, we can control every aspect of the parameters and easily accept the outcomes of the choices made. After all, if it fails, we can just reset it, retrain it and try again.

The issue is that the autonomous systems we are building are being put to use in the real world, a world so complex that we don't fully understand all of the possible ramifications. A world filled with paradoxes and hard choices. A world with severe consequences when something goes wrong.

SECTION 3

The issue is that the autonomous systems we are building are being put to use in the real world, a world so complex that we don't fully understand all of the possible ramifications. A world filled with paradoxes and hard choices. A world with severe consequences when something goes wrong.

Culture And The Absence Of Objectivity

Where does culture mix into these moral and ethical complexities? What we consider to be secure, safe and acceptable are often dictated by our culture. Our background, education and training have a deep impact on how we see our world. Our culture creates both perspectives and boundaries, and our behaviors, ideas and customs are largely grounded in the behaviors of those around us — as well as our blind-spots. We do not exist in a vacuum, and we are a product of the cultures we are immersed in.

If you can accept the premise above, we can add another layer of complexity: your particular culture is not unique, nor is it universal. There is no one, single culture. Instead, our world has countless cultures, with each culture influencing and being influenced by the individual members of that culture, with each individual member often a member of a number of cultures throughout their life.

Why is culture something to consider when working with autonomous systems and vehicles? One of the ideals in autonomous systems that is particularly evident in vehicles is that we can replicate the ethical and moral choices of humans and apply them globally. In other words, if we can identify the right rules, we can just program our vehicles to make the right choice every time.

This idea is clearly biased. One does not need to travel to many foreign places before they realize just how different humans are and can be. It takes little observation to recognize that groups of humans make their own rules, and very few, if any, such rules are universal. A recent study, *The Moral Machine Experiment*[87], makes this point extremely clear.

In a global survey of more than two million people, researchers found that there are a dramatic differences in how different cultures interpret situations and make difficult, ethical choices. In the example above, where you were faced with choosing who to sacrifice, there may seem to be an obvious choice for you. The choice may seem equally obvious for someone from another part of the world who is influenced by a different culture, only that may involve a different choice. What may seem to be the obvious "right" choice to you may be the equally "wrong" choice for someone else.

What happens then, if we choose to create universal rules for autonomous systems? Which rules do we select? Do we opt for the rules of the programmer who wrote the code, or the generally accepted rules of the country of the manufacturer? What then if the product is exported to a different culture? Do we allow the owner to choose how the system is making decisions, or do we require policymakers to regulate the rules for the industry? Or should we opt for a randomization algorithm where the system will choose from available options?

Your answers to these questions are likely to be different than mine. The answers you have are most likely a product of your cultures. Cultures have evolved over millennia as our societies evolved from hunter/gatherer, to farming, to the digital age, and as our societies changed, our cultures did too. Our cultures dictate which are acceptable behaviors, ideas and customs, and which are not.

Impact Of A Security Culture

Throughout time, a constant human concern has been dealing with threats. Back in the day, you may have been required a passcode to enter cities to ensure you were allowed entry. The Romans experimented with ciphers two millennia ago. Da Vinci created a secure communication device that would disintegrate the message if the wrong code was used to open the device. Modern technology requires us to use better security technology and more adequate practices than those we used yesterday.

Take cybersecurity for example — some may consider that cybersecurity is all about technology, while others consider cybersecurity to be both technical and cultural (people and process). You can test yourself right away by considering this: what is good authentication? Depending on your training and your exposure to security, you may decide that good authentication is *something you remember* like a password consisting of the name of your dog, or maybe the numbers 123456. Someone else may decide that good authentication should be a strong password, and that a strong password should be following certain rules[88].

Others may agree with the principle that a good password needs to be a strong one but disagree with the suggested rules to create a strong password, instead making their own. Your opinion depends on your culture.

Take someone who has a computer science education where the focus of the education was on building computer systems, with little education on secure programming practices and hacking techniques. This person is likely to have a

very different perspective and understanding of security than someone with a similar degree from a university focusing on cybersecurity. Their answer to the password question is likely to be different from each other.

Take these same two people and insert them both into either of two different organizations. The first organization is conscious about security and have training in place, use pair-programming where juniors work alongside seniors to ensure both knowledge transferal and quality assurance. This organization has systems in place to scan the code for API-keys, they have code reviews and they are constantly looking for ways to improve. They also have a policy that security related issues in code can halt a push to production, even if it means that the update or new feature will be delayed.

The second organization is focused on pushing new features fast. Each developer is given the power to decide where they want to work, including from home, and no structure of working together is enforced. There are no secure programming practices and no code review. Both organizations are happy with the status quo and see no reason to change their current culture.

In the first organization, it is likely that both candidates will follow a similar path and learn how to securely build products according to the culture of that organization. Most likely, both the candidates and the organization will benefit. In the second organization, one candidate is unlikely to learn anything except probably to focus on features over security. Over time, this person may come to think that security is not needed, or even an unnecessary complexity that gets in the way of them doing their job. The second candidate may at first be surprised at the poor security practices and may decide to quit, or adopt to their culture, or try to change the culture to improve security.

Research into age and experience[89] show that employees are better at security the older they get. At the time of the research, it was expected that people growing up today, with their access and exposure to new technology, would be more adept at understanding security. That hypothesis turned out to be wrong. Actually, when it comes to security culture, there is a clear social aspect that influences people. Older people got security better than younger people (they were all professionals), and even more interesting, but perhaps not so surprising, employees who have been working longer in the same organization had a stronger sense of security culture.

These findings can be explained by the impact culture has on people. As inherently social creatures, we adjust our behaviors, ideas and customs to those people around us based on our perception of what is acceptable and what is not. The longer a person is exposed to a particular culture, the more ingrained the culture becomes in the individual members.

Circling back to the two students above, it will take some time for them to adopt the culture of their new employer. Applying the findings from the research, employers who provide security training (especially with a good onboarding program), combined with mentoring programs where new employees get to work along with a senior for some time, are better at ingraining security culture in the new employees. Let us hope they both are working in a culture of innovation with a strong focus on security, especially if they are producing technology for tomorrow.

Conclusion

Autonomous systems and vehicles are created to solve real world problems. In doing so, they force us to examine humanity by challenging what we think we know about the world around us. It is easy to make a vehicle move straight ahead and follow a path — just develop some logic with a few rules and program the system to make the choice.

In a simple world, we can do just that: use simple logic to make simple choices. In a complex world, like the one we inhabit, what we consider simple choices may be far from that. That is good news, as it makes us look deep into ourselves, as a person and as a species. Do you sacrifice the child, the elderly pedestrian or the two passengers? Or, is there be an entirely different solution?

The role culture plays in both the development and security of autonomous systems is multifaceted and more complex than it may seem at first glance. Culture has a significant role to play in the process of creating and implementing autonomous vehicle technologies, and as such requires a deeper understanding of how it is helping to shape the future of these technologies.

Kai Roer is Founder and CEO of CLTRe, a security industry veteran, author and researcher. He specializes in security culture and serves as a strong voice advocating science and fact-based understanding of human factors that influence risk and security.

SECTION 3

Safety and Security Culture for Automotive Innovation

Adam Boulton, *Chief Technology Officer*
BlackBerry Technology Solutions

Building a software safety and security culture can seem like a daunting task because they are such specialized areas of engineering. This is especially true when you start going through all the impact scenarios of failures and overall risk management. So, when developing a safety and security culture, I believe the first thing to grasp is a deep understanding of the similarities and differences between these engineering disciplines. By doing so it will help instill the importance of these efforts and means a strategy can be put in place for creating harmony between both efforts. Ultimately, they strive to achieve the same goal of improving overall quality and develop forms of protection against particular scenarios.

The main difference between safety and security is the perspective. Typically, safety engineering is focused on protecting against unintentional behaviors whereby security engineering targets deliberate malicious behaviors. It is extremely important for organizations to recognize this because it plays a fundamental part in how resources will be utilized and the activities which will be carried out. Safety and security engineering is for the most part a union; they are not orthogonal concerns. With both disciplines, the activities span throughout the entire lifecycle of a product and both, like any quality improvement and risk management, work best when adopted as early as possible.

By drawing some precise parallels between the two activities, we can see the systematic analysis that takes place in activities such as HAZOP are similar to performing threat modeling. Both are performed to represent and manage risk and are completed at design phases. The same is true for fault trees and attack trees. These are two different terminologies and deductive techniques, but fault trees are typically applied for safety and attack trees within security. Whilst the overall technique is almost identical, it looks at things with a different perspective. It uses specific terminology to describe a fault or attack but still comes up with a conclusion of what can go wrong.

However, there are many areas in which safety and security have their conflicts. Where we tend to see the biggest impact on performance and usability can become significantly more challenging. Many areas within safety and security engineering revolve around non-functional security requirements — those aspects of the system that a user will be oblivious to. Some examples of this could be watchdog timers, compiler defensive technologies, permissions and all coding standards.

What is particularly interesting about non-functional security requirements is that they often require the most attention for collaboration between safety and security engineering. It's important to reach a fine balance. As an example, it may be that there are requirements to ensure that memory protections (RELRO, NX, stack cookies) are applied to all native binaries. However, this becomes extremely challenging for embedded systems. This is because each non-functional requirement will typically add an overhead, which in turn impacts the overall performance of the system. And this in itself is where the challenge and balance really lies. Embedded systems will have limitations on hardware performance due to factors such as budget constraints or physical limitations of the device.

These nuances between the safety and security disciplines are important. Knowing which activities play well together allows teams to maximize their output but also know when the activities will conflict. However, a good general rule to follow is "safety first," the rule we're all taught from a young age. But at the same time recognize that a system cannot truly be safe without security.

Adam Boulton is the Chief Technology Officer and Senior Vice President of Product Security. He's also the Inventor and Chief Architect of BlackBerry Jarvis, a powerful binary static analysis SaaS tool, which delivers innovative and advanced capabilities in software security analysis.

SECTION 4

Widening the Road Less Traveled

SECTION 4

Connecting the Dots: Transportation Management Systems, Connected and Autonomous Vehicles

Marsia C.Marisa Ramon, *Senior Research Engineer*
Victor Murray, *Group Leader*
Southwest Research Institute

As part of the Intelligent Transportation System (ITS), the modern transportation management system (TMS) consists of numerous devices. These include traffic signal controllers, dynamic message signs, road-weather information systems and other IP-addressable devices. Nationwide, these deployments vary dramatically from state to state or even between management centers. However, their architectures all work with common components and subsystems with the goal of facilitating safe and efficient traffic flow while providing operators with traffic and environment information. The systems provide this information to both traffic management center (TMC) operators who make traffic management decisions, as well as directly to the driving public through signage and public websites. Some of these systems are just beginning to identify and manage cybersecurity risks inherent to the distributed nature of their networks. It is important to understand and prepare for the additional cybersecurity challenges TMS will face with integrating connected and autonomous vehicle (CAV) services.

By understanding the traffic and environment conditions, traffic managers can improve the safety and mobility of the roadways. To maintain public trust while keeping roadways safe and operational, state and local agencies must consider the cybersecurity of the field components and implement a plan to protect networked field components and the data they communicate.

Many advanced traffic management systems (ATMS) use devices that implement standard protocols in compliance with National Transportation Communications for ITS Protocols (NTCIP). Initially, this communication standard was not developed with cybersecurity in mind or to or to protect networks field systems' and components' communications. This is done through several cybersecurity-related steps, including

SECTION 4

overall and specific cybersecurity agency guidance. These actions perform assessments of risks posed to the technologies and provide strategies to explain how to mitigate vulnerabilities common to field architectures.

With the advancement of vehicle-to-everything (V2X) technologies, including vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), the already data-rich TMS environment will contain even more information for both good and bad intentions. So, while the additional data will provide TMC operators, the public and connected technologies the information to operate with improved safety, it will also provide potential attackers new avenues for service disruption, public embarrassment and the ability to introduce false data.

Cybersecurity Risk Management Of TMS Field Networks

There are over 300,000 traffic signal systems across the United States with over 2,000 added each year. Each contains different levels of network access and embedded security. Originally, the TMS field systems only supported analog or serial communications. Over time these systems have been attached to IP-based networks or replaced with IP-capable devices to enhance the safety of our roadways and support a cooperative environment. Now these IP-capable systems communicate back to ITS business networks to relay traffic and weather conditions. While the communication medium may change several times, the underlying NTCIP protocol remains, making it critical to secure these devices.

Developing Guidance Through Coordinated And Collaborative Research

In 2017, the Transportation Research Board (TRB), a unit of the National Academies of Sciences, Engineering, and Medicine, saw the need to assist state agencies in understanding the cybersecurity risks posed to ATMS. The board also wanted to provide guidance on first steps state agencies may take to improve their cybersecurity posture. For this purpose, TRB selected Southwest Research Institute (SwRI) to lead a two-year program under the National Cooperative Highway Research Program (NCHRP). This research into cybersecurity weaknesses in Transportation Management Systems (TMS) resulted in guidance for securing ATMS and best practices for integrating connected and automated vehicles (CAV). This program consisted of five tasks:

1 Development of the *Literature Review and Ongoing Efforts Security Analysis Report*. This task captured information that applies to standards and efforts related to cybersecurity in transportation.

There are over 300,000 traffic signal systems across the United States with over 2,000 added each year. Each contains different levels of network access and embedded security.

2 Risk assessment of typical TMS design. This task assessed risks for 17 field device categories used in transportation (e.g. traffic signal controller, changeable message signs, road side units, etc.)

3 Adversarial assessment of high-priority systems. High-risk device categories underwent penetration testing.

4 Cyber-attack response guidance development and workshop. Creation of a cybersecurity web guidance tool to help transportation managers assess the state of their cybersecurity.

5 Cybersecurity and privacy primer for the deployment of CV and AV technologies. This document looked at how CAV will impact transportation systems.

At the time of publishing this article, the results from Tasks 2 to 5 have not been published by the Transportation Research Board.

SECTION 4

Securing A TMS Environment — Where To Begin?

As organizations work toward securing the TMS and implementing best practices and standards, the World Health Organization (WHO) recommends establishing a cybersecurity program as described by the 2017 *NIST Framework for Improving Critical Infrastructure Cybersecurity* (draft 2). This framework comprises three parts: The core, the implementation tiers and the profiles. The framework core describes the risk-based cybersecurity management activities and desired outcomes common across critical infrastructure sectors. The framework implementation tiers define characteristics of how an organization views cybersecurity risk and, given the processes the organization has in place, how agile and risk-informed they are. Finally, it provides alignment based on the requirements, financial needs, risk tolerance, and standards and best practices. Together these parts will provide overall cybersecurity risk management guidance at a TMS organization level and assist when managing cybersecurity risks associated with field systems.

Focusing on the field network system level to protect both devices and data, security managers may incorporate the NIST Risk Management Framework (RMF) into the secure life cycle (SLC) process, security standards and policies. Some of the cybersecurity and risk management standards and guidance documentation used when providing direction include:

- NIST Cybersecurity Framework
- NIST Risk Management Framework
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27005:2011 Information Security Risk Management
- ISO/IEC 31000:2018 Risk Management Guidelines
- NIST Security and Privacy Controls for Federal Information Systems and Organizations
- NIST 800-37 Guide for Applying the Risk Management Framework
- NIST 800-39 Managing Information Security Risk
- NIST 800-53 Rev.4 — Security Controls Catalog/Assessment Procedures
- Guide for Assessing the Security Controls in Federal Information Systems and Organizations
- Federal Information Processing Standards (FIPS) 199 — Standards for Security Categorization
- FIPS 200 — Minimum Security Requirement

Active participation in the standards community (e.g. NTCIP, Society of Automotive Engineers (SAE), Institute of Electrical and Electronics Engineers (IEEE), IEC and ISO) helps to understand how and where to apply cybersecurity standards and guidance when examining TMS field networks. Following these standards and processes can assist in generating a cybersecurity risk management and response plan, and provide standardized methodologies and metrics to assess the risk of ITS field networks.

To understand how the RMF process works, we must first consider the Secure Life Cycle (SLC) process. The SLC consists of four steps: identify, assess, protect and monitor, as shown in Figure 3.

The SLC steps include:

1 **Identify** — Understand what needs protection by mapping out field systems and components, starting with a high-level network map then adding detail.

2 **Assess —** Perform a security assessment by prioritizing the field systems, identifying risk and exposure to them and finding vulnerabilities to create a security baseline.

3 **Protect —** Bring TMS field systems and components up to state and local agency security policy standards, and configure the systems to mitigate or eliminate vulnerabilities.

4 **Monitor —** Continuously evaluate the field systems and components to ensure that the security measures and controls put in place remain in place in the event of an attack. Have a response plan in place to limit the exposure.

By incorporating the SLC process, the RMF process links field device security with organization security. The RMF consists of six steps: categorize, select, implement, assess, authorize and monitor, shown in Figure 4. Several of the steps overlap with the SLC process so aligning the two processes provides a breadth and depth of coverage of the TMS field network security posture.

The steps to perform the RMF include:

1 **Categorize —** This step coordinates with *Identify* in SLC. Use high-level architecture documents to gain a clearer picture of the risks identified to field systems and prioritize them based on their impact to the TMS.

SECTION 4

2 Select — Choose what security controls or safeguards to implement based on how they address confidentiality, integrity and availability of the TMS field components. Then, create a security baseline. Last, tailor the selected controls to each agency's requirements and policies.

3 Implement — Put the selected security controls in place to begin minimizing risk to the TMS field network. This step is similar to Protect in SLC, except it suggests to begin protecting the system earlier in the process.

4 Assess — In line with the SLC, use security assessments and penetration testing to determine if security requirements are being met. In addition, verify that the security controls operate as intended. This provides a good measurement of the field network's baseline security posture and provides security control cost-benefit comparison.

5 Authorize — Address the need to ensure that access to the field network is granted based on operational needs. This is in addition to developing an understanding of the risk associated with the possibility of a field component becoming compromised.

6 Monitor — Like the SLC, this step recommends an ongoing evaluation of security controls and documented changes plus conducting security impact analysis of the changes and reporting the security state.

As development and deployment varies dramatically between both state department of transportations (DOTs) and TMCs, large and small organizations can align the basic SLC process and the RMF process to develop their own customized risk management framework. Doing so will improve or develop a baseline of their field network security while making the field network more resilient to cyber-attacks. Departments can align the SLC and RMF by performing the following security assessment activities:

- **Map the field network to generate a high-level architecture model.** Categorize the field systems and components by classifying and understanding the following:
  - How data is processed, stored and transmitted by TMS field equipment
  - The potential impact of data to the TMS infrastructure
  - What, if any, baseline security controls are in place
- **Identify high-priority attack threats against the field network.** Identify high-priority risks through:

Figure 3. Secure Life Cycle (SLC) process

Figure 4. Risk Management Framework (RMF)

  - Access to business network via unmonitored roadside cabinets
  - Default passwords for TMS networked devices
  - Third-party access to a business network (e.g. news access to cameras)
- **Evaluate, prioritize and mitigate risks.** Recommend mitigation and attack response strategies to reduce incident exposure such as:
  - Install tamper detection hardware in high risk roadside cabinets
  - Institute polices to maintain and rotate networked device passwords
  - Install tripwire monitoring software on third-party access points

Understanding Threats Against One's System

Creating abuse or misuse cases simply involves creating lists, attack trees or diagrams depicting interactions between field systems, components and TMS business networks to decipher a goal from an attacker's perspective. For example, an attacker may gain unauthorized access to a trusted device or application, and then use it to send a false message. When the motorist sees it on a DMS sign, it causes them confusion or distraction.

SECTION 4

It is good practice to include public sources of vulnerability sharing to develop a thorough list of cybersecurity attacks that apply to field equipment, installed configurations and protocols. (One example of this type of source is NIST's National Vulnerability Database.) The following common vulnerabilities have been discovered in various industries:

- Login vulnerabilities (i.e. default, blank or weak username and passwords)
- Unsanitized data inputs (e.g. SQL injections)
- Extensive user and group privileges (e.g. unneeded privileges granted to one user, device only has admin or root account)
- Denial-of-service attacks (e.g. communication traffic flooding, data buffer overflows)
- Unpatched systems (i.e. active exploits exist against deployed versions of field equipment)
- Unencrypted sensitive data at rest and in motion (i.e. how securely is data stored and transmitted)

When considering the vulnerabilities listed above, the most prevalent ones should be eliminated as determined by how easily exploitable they are, how large of an impact they pose to the TMS networked systems and which ones would cause the most embarrassment.

As part of the threat modeling activity, leveraging threat information across critical infrastructure domains such as automotive, transportation and energy, can identify prevalent attack threats and vulnerability exploits. Knowing the threats against the TMS field equipment, operators can perform analysis to assess the impact to the TMS field network. This helps understand if data was disclosed, altered, destroyed or unavailable. After identifying threats and risks to the TMS field network, the next step is to compile a list of security controls, safeguards and countermeasures, and identify their effectiveness in mitigating or reducing the risk.

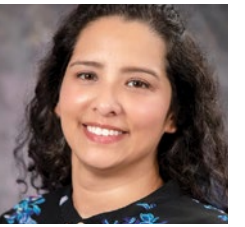
Identified risks to the TMS field network are then evaluated using tailored risk ratings. In determining risk to field equipment, it is important to use standards and well known classification schemas (i.e. NIST Risk Determination in *NIST SP 800-30 Rev. 1 — Guide for Conducting Risk Assessments* or Microsoft's *Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability (DREAD)).*

Documenting risk involves describing the risk, including the field device (asset), vulnerability and the threat that exploits the vulnerability. For each attack threat, perform an investigation to determine if the field device or system suffers from vulnerability. As an example, a risk-based approach to prioritizing risks includes assigning the severity of the vulnerability or threat and the likelihood of the threat occurring. Determining risk rating helps guide the security assessment to address the issues with the highest concern and impact. This information is then used to guide an adversarial assessment or penetration testing to evaluate the most critical paths in the TMS field networks.

Adversarial assessments and penetration testing can be performed both during the Assess step of a RMF and during the *Monitor* step. This is because performing this test provides verification and validation of implemented security controls.

Performing the security assessment, that contains SLC and RMF processes, will then help develop risk-based guidance that will provide state and local agencies direction for attaining and maintaining the desired level of security over the life of the TMS and beyond.

Marisa Ramon is a Senior Research Engineer at Southwest Research Institute (SWRI). She has lead several cybersecurity risk assessments, including threat and vulnerability assessments, developed automated technologies and performed penetration testing of cyber-physical systems.



Victor Murray is a Group Leader in the Intelligent Systems Division at SWRI. He is a Certified Information Systems Security Professional (CISSP®) whose background includes performing risks assessments, penetration tests and developing secure systems.

SECTION 4

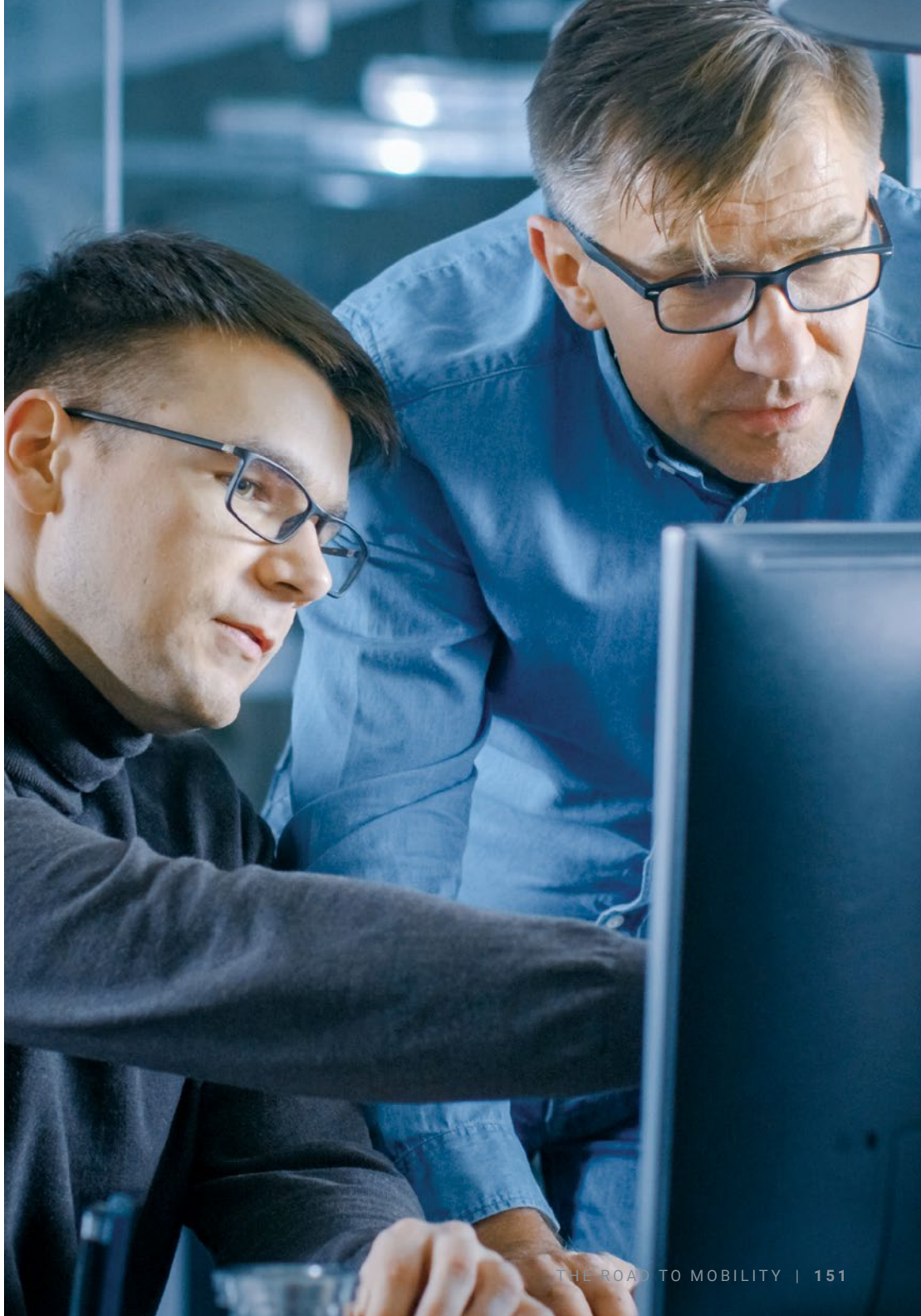
Swimming Upstream: Securing Automotive Supply Chains Against Cybersecurity Threats

Ken Obuszewski, *Director, Business Development*
BlackBerry

With the constant news around cyber-attacks, it can be very daunting for CISOs, CSOs, CIOs and engineering VPs to put in place plans to address cybersecurity threats for all their products across the software supply chain. Automobiles are a very pertinent example of the challenges posed by cybersecurity threats to complex software systems. This is especially true with the onset of ubiquitous connectivity and the move towards autonomous vehicles, Intelligent Transportation Systems and transportation as a service.

In a recent study on automotive cybersecurity practices performed by the Ponemon Institute[90], 30 percent of the respondents do not currently have a product security team or program in place, and 63 percent test less than half of their products and technologies for vulnerabilities. This is aligned with BlackBerry's information[91] in which only 29 percent of people cite a central security team within their organization and 23 percent do not currently have a security infrastructure in place.

Vehicles provide a particularly challenging environment for cybersecurity. Some of the issues include very complex software with over 100 million lines of code in a "network on wheels" of distributed computers, a complex supply chain and very long lifecycles for software in the vehicle. The last point means that the software will inevitably be out of date and must be updated to address the latest vulnerabilities and stay ahead of bad actors. Even with these known issues, the Ponemon study identified that only 44 percent of organizations surveyed impose security requirements on their suppliers, despite that 73 percent expressed a high or very high degree of concern on the quality of software provided by their third parties.



SECTION 4

Often with a new challenge, the biggest hurdle is taking the first step, but it is nevertheless imperative that carmakers make the necessary investments to secure their vehicles. The 2015 Fiat Chrysler Jeep hack is still the most visible illustration of the risks associated with inadequate security. It involved a recall of more than 1.4 million vehicles with significant direct costs to Fiat Chrysler Automobiles and a public relations firestorm for the company and its supply chain. One report[92] estimates the total cost to Fiat Chrysler Automobiles could have approached $1.4B.[93] The same report also revealed a 600 percent increase in automotive attacks over the last five years, and that Black Hat attacks in automotive overtook White Hat activity for the first time in 2018. Twenty-eight percent of these attacks involved the unauthorized control of vehicles. This will become an ever more serious threat to society as autonomy advances and drives home the notion that safety and security must be addressed with a holistic strategy.

When it comes to addressing these challenges, BlackBerry has found success using a Secure Software Development Life Cycle Process (S-SDLC), with a three-phased approach:

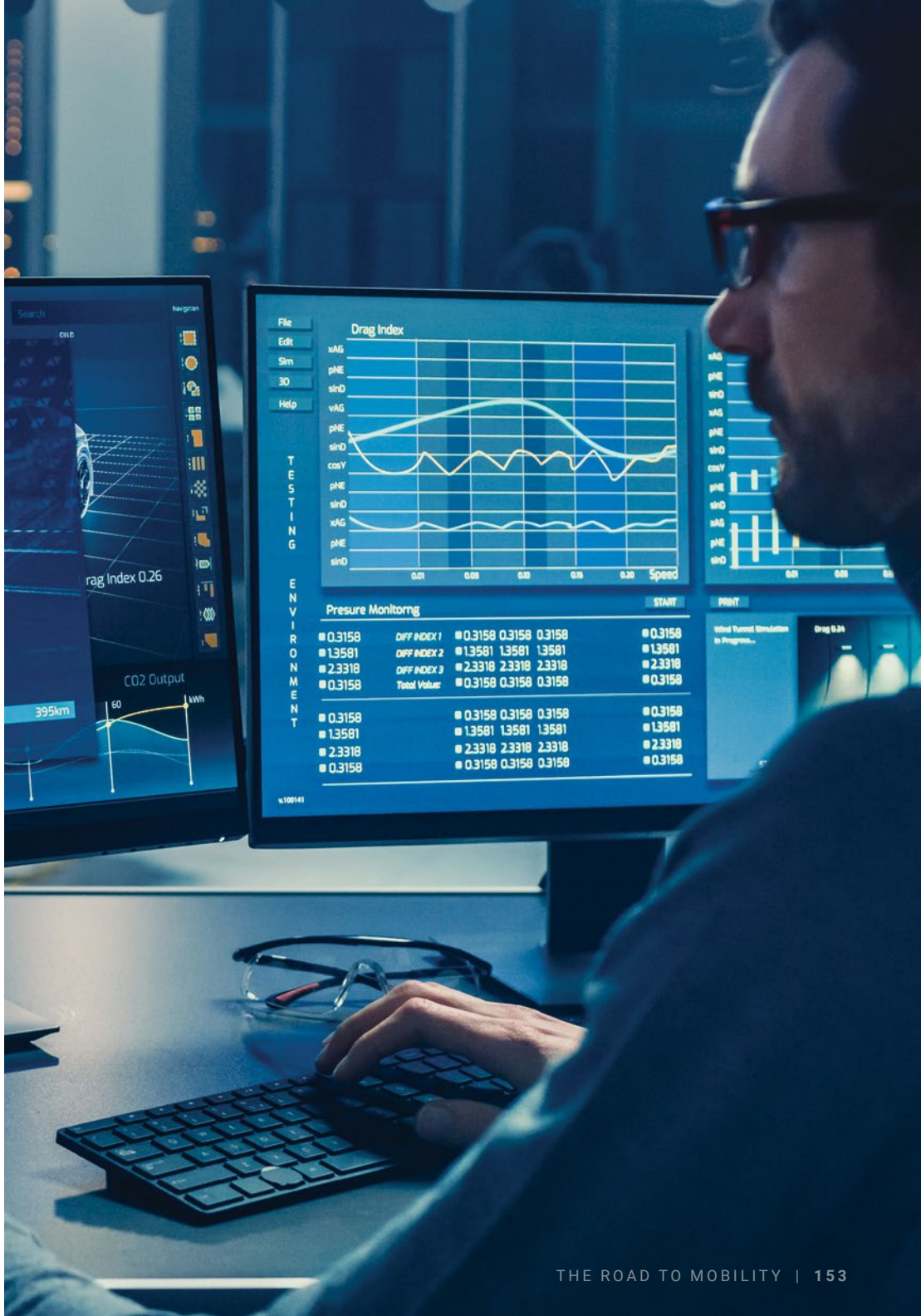
1. Assessment
2. Implementation
3. Continuous improvement

Assessment

The obvious, yet significant, first step is to take stock of all current software assets, software development and security practices and to identify the desired state. Major steps in the assessment phase include:

1. Use an industry model to assess your current security practices

BSIMM (Building Security In Maturity Model) or Open SAMM (Software Assurance Maturity Model) are good examples to consider. BSIMM represents a community study involving 120 companies across multiple verticals providing a public cybersecurity framework. Open SAMM is an OWASP (Open Web Application Security Standard) project designed to be flexible based on the individual needs of organizations.



SECTION 4

2. Establish a baseline profile of your software assets across your internal and external supply chain, including a vulnerability assessment.

Understanding the software bill of materials (BOM) is a critical and often ignored step in assessing a security profile. In a modern electronic control unit (ECU), it is typical to have more than 100,000 files with multiple runtime environments and archives. It is even more critical with the proliferation of open source software (OSS) and the associated CVE (common vulnerabilities and exposures). OSS also brings the challenge of general public licensing (GPL) compliance.

3. Define the desired security process, based on your risk tolerance, and lay the foundation of a strong security culture.

BSIMM and Open SAMM allow an organization to build the framework of their security strategy and benchmark against industry peers. This requires companies to build the infrastructure of a cybersecurity organization. An organization that implements a S-SDLC for the first time may initially use an external consultancy. However, it is critical to establish the proper internal expertise and ownership. This includes an executive with ultimate responsibility for security in the company or organization. A "Center of Competence" concept can be employed, whether the resources report to this leader or not.

Implementation

As an organization moves from assessment to implementation, it is critical to build cybersecurity into the culture of the organization, and to integrate it into the development and deployment processes. Cybersecurity and software quality standards need to be translated to a set of key performance indicators (KPIs). This is so they can be measured and enforced across all development teams, whether internal to the organization or across the software supplier base. The ability to measure progress is critical for a quantifiable software security strategy. It is important to move away from a "leap of faith" approach, whereby organizations believe they must be getting more secure simply because more is being invested.

A wide set of standards exist that can be deployed as part of your S-SDLC. These include community-based databases and common coding standards, such CWE and multiple SEI CERT variants, as well as industry-specific versions such as ISO 26262 for automotive and IEC 62304 for medical devices. Also, of critical importance is to measure the adherence to software craftsmanship best practices such as the implementation of compiler defenses and secure APIs to prevent attackers from exploiting memory corruption vulnerabilities.

The final implementation step is to automate within the build and continuous integration processes. It is recommended to integrate directly within the automated build process.

The implementation phase requires a business to continue to grow and enhance the capabilities of its cybersecurity team. This includes providing oversight, with decision-making authority, for the security team and moving from reactive to proactive security engineering. An example of proactive engineering would be to build a cybersecurity capability maturity model.

Continuous Improvement

Once the implementation infrastructure is in place, the next step is to drive continuous improvement. This requires the ability to track vulnerabilities and software quality over time, both at a product level and at the organizational level. Automated tracking mechanisms will allow a development team lead to ensure that their projects are tracking to success, and to identify potential issues at an early stage. It also provides a mechanism to audit suppliers. Most importantly, it drives a culture and a process to push accountability all the way to the source, the developer, as over time adherence to the defined standards will become second nature. Nevertheless, this never becomes a static process as one must continuously evolve to stay ahead of attackers and to embrace the latest best-in-class practices.

Ken Obuszewski is BlackBerry's Director of Automotive Business Development. He's built and leads a team of global domain experts that span the QNX safety OS and hypervisor, cybersecurity and acoustics technologies.

SECTION 4

Technology Choices for OEMs

Kaivan Karimi, *Senior Vice President and Co-Head, BTS Sales*
BlackBerry

Today's cars have millions of lines of code that manage increasingly sophisticated systems. The quality of this software has everything to do with the overall safety of vehicles. To underscore safety, engineers have to prove the quality of code and how it performs in order to certify that the vehicle as a whole will perform at a reliable level of safety. Part of this requires detailing how the code is developed and by whom. This increases the confidence in the safety performance of the car while also reducing the liability of automakers.

Despite the ISO 26262 standard, software certification in the automotive industry is immature compared with other safety-critical domains, such as healthcare. As we point out in another article in this guide, "Keeping Safety at the Forefront of Automotive Advancements" by Yi Zheng, building a car based on high-performance safety standards requires a team of professionals with this expertise. However, because this level of safety standards is new to automotive, there are few experts who have an intimate understanding of what it means to build functionally safe software for cars.

Transplanting Expertise

BlackBerry has worked across a broad range of sectors such as nuclear power plants, surgical robots, class III life-critical medical devices (ie: Intuitive Surgical's Da Vinci Surgical robotic device) and more. We have served non-automotive industries for over 35 years, powering solutions for global companies like Cisco, General Electric, Intuitive Surgical, Lockheed Martin and Siemens that require safety, reliability and security.

Certain standards such as IEC 62304 in medical devices have stringent requirements related to producing risk analyses. Such analyses include traceability of patch sets and code as well as ensuring that the development processes are strictly followed. These tasks can be quite difficult and time consuming to do, but they are critical to the reliability and performance of the devices. The process directly applies to the automotive industry as well.

SECTION 4

Currently, our safety-certified, secure foundational automotive software is used by over 45 automakers and in more than 150 million vehicles on the road today. For well over three decades, BlackBerry's micro-kernel QNX® technology has powered many of the world's most mission-critical embedded systems including nuclear power plants, industrial controllers, surgical robots and class III life-critical medical devices — the types of systems that are required to operate safely, securely and reliably, 24 hours a day, 365 days a year, without failure.

Our ability to deliver safety certification and security in other industries has successfully transferred into the auto industry. BlackBerry has been involved in 290 startup productions and delivered a 100 percent success rate — a record that's unlikely that anyone else in the industry can match. We understand what it takes to deliver software to an environment that can't afford to have a failure.

The Dangers Of Open-Source Software

Linux® is generally touted as a "free" operating system, and, in certain regards, this is indeed the case. For the most part, you can download the source code to all components of the Linux distribution or "distro" (that is, the operating system, drivers, utilities, tools, libraries and so on). After all, Linux originated as a hobbyist-level effort to come up with a free version of Unix, and belongs to the general class of software known as "Free Open Source Software" (FOSS).

> **Our ability to deliver safety certification and security in other industries has successfully transferred into the auto industry. BlackBerry has been involved in 290 startup productions and delivered a 100 percent success rate.**

Linux is maintained by the Linux community, which includes hobbyists, volunteers, academic institutions, commercial hardware vendors and commercial support organizations, to name a few. You're free to modify any part of the Linux system you see fit, create a product and sell it. In this respect, Linux appears to have a cost advantage, in that there are neither source code nor end-product licensing costs.

However, considering only those costs gives an incomplete, and therefore skewed, analysis of Linux's total cost of ownership. A better way to think about it is that Linux is free like a free puppy. Anyone who has a dog knows the never-ending expenses that pet ownership can entail, from veterinarian bills to food costs to the time invested for training — together, these represent the true total cost of ownership of a puppy. Likewise, the total cost of ownership for a "free" Linux OS includes the extra effort and testing needed to certify a system that uses an open source OS, the cost (or revenue lost due to delays) in bringing the device to market, and the investment needed to sustain an in-house team of OS experts.

It is critical when evaluating the investment of an OS to include such big-ticket items as development, maintenance, support and opportunity costs — not to mention the fact that by building your own Linux distro, you end up with a build of the OS that is unique to you. Also, the contribution to the TCO of Linux's licensing model, the GNU Public License, (GPL for short), is a significant factor.

Certifying Linux Code

As an open source solution, Linux encourages many people to make contributions and changes to the source base. Since tracking began 10 years ago, over 12,000 developers from more than 1,200 companies have contributed to the Linux kernel. This causes a problem for potential automotive customers in that many simply will not buy a system unless they can trace everything, including the OS, back to its original sources. The sheer amount of contributors to Linux's source code makes this virtually impossible and extremely time consuming.

This is where a micro-kernel architecture brings big benefits. A patented system can trace every build back to source origins and specific commits. The lineage of all source code is known and tracked.

Another issue with Linux is the ripple effects caused by changes to the source code. A small patch or software update may result in a large ripple of rebuilds and changes that could be an expensive retest and recertification effort for embedded or safety certified devices. The Linux Foundation estimates that the development community has been merging patches at an average rate of 7.71 patches per hour since the 3.10 kernel release (October, 2011). Keeping up with this rate of change in terms of accepting or rejecting the patch, validating the ripple through effects of the change (e.g., dead code), and testing is a monumental task.

SECTION 4

Managing The Overhead Of Ownership

In the spirit of open source, there are numerous versions of Linux that have been created by users to meet their needs. Users create unique versions of tools, libraries, drivers or even operating system components. The important realization, as it relates to the total cost of ownership, is that if you're coding using Linux for your application, it now becomes your job to configure, build, support, certify, test, and maintain a large code-base that is the foundation of your product.

On top of all of this, you now need to hire Linux experts just to provide those functions, let alone the developers you need who are actually concerned with your product proper. And, not just "generic" Linux experts — a medium to large project might require such diverse skill-sets as kernel, GUI, middleware, drivers, networking stack, and so on which are often hard to find, let alone skills that a single individual has. When you add the maintenance burden of a multi-million line Linux distribution to your workload, you suddenly require all kinds of additional expertise that would not be otherwise required.

Once you've adopted Linux, you are on your own — it's up to you to ensure that you are using the correct licenses, and that you've attributed them properly. This isn't just a simple matter of duplicating the copyright notice in an appendix — an inadvertent "copy and paste" of open-source code can result in contamination of your proprietary source base.

> **When you add the maintenance burden of a multi-million line Linux distribution to your workload, you suddenly require all kinds of additional expertise that would not be otherwise required.**

Because of Linux's "community" development model, it's often difficult to know where to turn to for help. Volunteers, who have experience ranging from newbie to kernel expert, across one or more systems, do most of the Linux support. If you're lucky, there might be an available expert able to help you out. Unfortunately, though, timeframes are chaotic — an expert may help you immediately, or your issue may be sitting for weeks on end. Worse, the answer to your issue might be "upgrade to the latest version" or "apply this patch" — both of which are fertile ground for additional support issues.

Benefits Of A Micro-Kernel Architecture

BlackBerry has a broad portfolio of products and services to protect vehicles against cybersecurity attacks. We also have a wide range of functional safety-certified software with a micro-kernel architecture, such as our QNX operating system, hypervisor, development tools and middleware for autonomous and connected vehicles. Our software has been deployed in critical embedded systems for over three decades and has been certified to the highest level of automotive certification for functional safety with ISO 26262 ASIL D. As a company, we are investing significantly to expand what we offer in safety and security product and services. Simply put, this is what our customers demand and rely on from us — a safe, secure and reliable software platform.

In contrast to Linux, our microkernel QNX architecture provides an extensive level of fault containment and recovery so that every driver, protocol stack, filesystem and application runs outside the actual kernel, in the safety of memory-protected user space.

Intelligent Transportation

To create a truly connected transportation network means looking at how to apply advanced technologies — electronics, communications, computers, control and sensing devices — across all kinds of transportation. This goes beyond just cars, and extends into bicycles, scooters, and the signals and monitoring systems that manage traffic flow. In order to create a society that delivers advanced transportation options that everyone can trust, every part of the infrastructure has to be built to the same level of safety and security. It's not a pick-and-choose scenario; either everything is built to the same high-standards of trust and reliability, or none of it is.

As Senior Vice President and Co-Head of BlackBerry Technology Solutions, Kaivan Karimi drives the growth of embedded software and cybersecurity-related solutions for mission-critical applications in automotive, medical, defense and industrial markets.

SECTION 4

Digital Transformation Lessons for the Automotive Industry

Val Mukherjee, *Chairman and Founder*
Cyber Future Foundation and Constituents

Everything Matters

As various other sectors have realized the need for stronger cybersecurity, the automotive industry is waking up to the related risk, issues and challenges. Automotive has seen an aggressively escalating exposure with an intricate, and fast-growing labyrinth of connected vehicles and devices.

As with other sectors, it is becoming obvious that this is not a technology problem. The cybersecurity issues need a comprehensive overhaul of the ecosystem that encompasses people, process, technology, framework, automation, supply chain, third party participants and policy. Treating technology with technology only creates a patchwork of vulnerabilities that further complicates the issue.

While many learnings are common, there is something unique about the nature of cyber issues in the automotive industry. Security cannot be addressed alone. Instead, the answer requires an equal — if not greater — treatment of safety and privacy. It becomes ever more important to the cyber functions to seek the best practices and lessons learnt from other industry sectors. Translating them into the automotive environment allows those involved to skip the wasted effort and valuable resources that would come from reinventing the solution.

The Talent Gap

Talent is a burning platform for cybersecurity. Industries struggle to find, recruit and keep good talent. This shortage only aggravates the cybersecurity challenges posed by the digitally connected environment in which we live. It would be worth the effort for leaders — from OEMs to suppliers — to invest in cybersecurity talent specific to automotive.

SECTION 4

While the financial services sector has led addressing cybersecurity issues, it has not realized the result it desires. It is true that higher and more competitive compensation has started to attract more talent to the general field. However, it is still fraught with systemic talent-sourcing challenges, which includes the perception of it being a technology-intensive field.

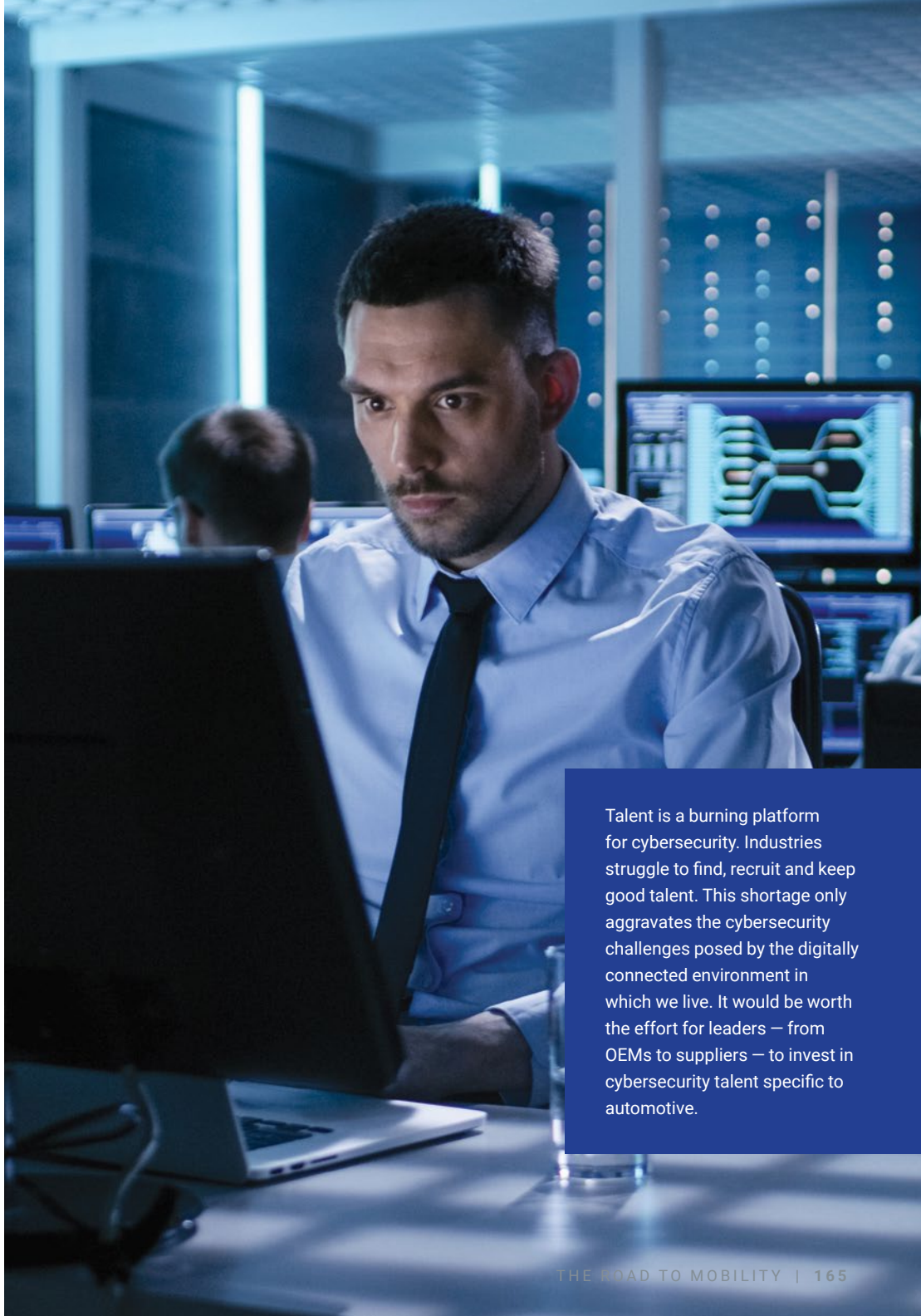
The automotive sector would do well to learn to not only make it financially attractive, but also promote diversity in the talent pool. The industry not only competes with other categories but also with other competing domains that are more diverse and experience-rich. The industry must start aggressive in-sector-specific talent development if it wants to have a fighting chance. This starts with teaching and training cybersecurity skills very early at the entry-level workforce. From there it must become an exciting proposition for the most junior cybersecurity workers to be interested and vested in a career in automotive.

Adaptive Process

The automotive sector, like other traditional sectors, is akin to follow tried and tested processes. While this does not seem to be a bad idea on the surface, 'We have always done it this way,' hurts the chances for success in a dynamic and ever-expanding world of connected vehicles. Thorough and frequent assessment of cybersecurity posture, programs, processes and practices are essential to ensure the proven methods remain relevant and effective toward addressing growing and changing demands. While most of the cybersecurity processes focus on IT, it's a recent realization that the product side is quite distinct and needs to be specifically addressed. Just as other industries have developed specialized processes, automotive needs to have a set of standard processes leading up to a holistic and comprehensive cybersecurity process portfolio for effective controls in both enterprise and product.

Technology

Technology innovation in the automotive sector is at its best and worst. The rate at which it is disrupting the business model is evident from the rise of ride-hailing apps, expansion of electric-powered, connected vehicles and the market adoption of autonomous driving in various forms and levels. This has been only a façade. Technology innovation has been faster than any other sector and has disrupted the industry from all ends — consumer to enterprise.



Talent is a burning platform for cybersecurity. Industries struggle to find, recruit and keep good talent. This shortage only aggravates the cybersecurity challenges posed by the digitally connected environment in which we live. It would be worth the effort for leaders — from OEMs to suppliers — to invest in cybersecurity talent specific to automotive.

SECTION 4

What is not obvious, though, is how deeply embedded technology has become on the product side. Any vehicle produced around 2008 and after is connected from the get go. It is now a difficult job to retrofit the millions of vehicles on the road. It's equally, if not more critical, to ensure the security of the millions of new vehicles getting on the road.

Now the automotive sector has to not only address the enterprise aspect of cybersecurity but that of millions of vehicles that are either on, or soon-to-be-on, the road. This calls for a solid product security program for the automotive sector from the OEM, Tier 1…X suppliers for both hardware and software. This proves challenging because other industries have not laid out a perfect path to follow. Product security has been an Achilles heel for the cybersecurity industry, which is coming to grips with enterprise and consumer applications. Healthcare device is the only other sector closest to having any reasonable attention to product security, but it has issues of its own.

However, there is hope in that connected devices in general, and automotive product security in particular, have generated great enthusiasm amongst those entering the field. This level of excitement only increases as the sector opens up new challenges, and thus doors, on which cybersecurity talent can focus.

Beyond product security, the industry could well draw mature practices of enterprise security from other groups and align them to automotive needs. Doing so would help technologies in traditional industry provide opportunities to scale up to the level needed for automotive. This includes strong end-point protection, intrusion/threat detection and response, solid cloud security practices and digital identity provisioning capabilities, to name a few.

Automation can fill gaps that are prevalent in cybersecurity technologies and processes as well as provide the necessary augmentation to the talent gap. With automation and artificial intelligence, the auto sector can develop consistent and scalable platforms that will take on the challenges associated with a connected environment.

Frameworks

Cybersecurity has provided a common baseline for the overall capability and maturity for security functions, but has lacked nominal standards. It took a while for the industry to understand, define and develop a framework that could be adopted disparately, yet measured, compared and contrasted. For most of the industry, the NIST Cyber Security Framework has been the go-to common language of defining, implementing and operating capabilities. The rest of the industry has realized the power of frameworks that provide a common baseline and semantics to adopt, deploy and operate in a dynamic connected environment. This is one of the greatest learnings from the prevailing sectors. It is imperative, though, that automotive develop a sector-specific framework that could serve as the blueprint. Several efforts are on the way from different standard-making bodies including NIST, SAE and ISO. The sooner a framework is adopted the faster we can preempt the development of proprietary pockets of vulnerable technologies.

Frameworks are not only applicable for cybersecurity, but also privacy and regulatory requirements. Automotive cybersecurity will be impacted by both current and anticipated regulatory frameworks, some of which are currently being developed. We need to consider the potential requirements and help shape a regulatory framework that would enable a safe and secure vehicle ecosystem.

Securing The Ecosystem

An overall ecosystem view must be considered while also addressing the cybersecurity needs of the automotive sector. One of the critical aspects is supply chain, both of information and products. Measures have to be taken to secure the entire supply chain through a set of common adoptable controls. Because a host of third parties are involved in producing a vehicle, it's necessary to ensure that these software, product and service providers are equally prioritizing cybersecurity.

These are exciting times for a traditionally stagnant industry to join the technology revolution that started with digital transformation. While the path ahead is long and arduous, as long as the automotive sector learns from the lessons of others, our roads will be safer tomorrow than they are today.

As the Founder and Chairman of Cyber Future Foundation and Davos Cyber Future Dialogue, Val Mukherjee is a globally renowned cyber executive. He works as a Managing Director for Cybersecurity Advisory at EY.

Endnotes

1 United States Department of Transportation Bureau of Transportation Statistics. Accessed September 6, 2019. https://www.bts.gov/content/commuting-work

2 https://www.npr.org/2018/09/20/650061560/stuck-in-traffic-youre-not-alone-new-data-show-american-commute-times-are-longer

3 Sivak, Michael and Schoette, Brandon. *Recent Decreases in the Proportion of Persons with a Driver's License across all Age Groups*. University of Michigan Transportation Research Institute. January 2016.

4 Sivak, Michael and Schoette, Brandon. *The Reasons for the Recent Decline in Young Driver Licensing in the U.S.* University of Michigan Transportation Research Institute. August 2013.

5 https://www.cmu.edu/metro21/

6 https://www.cmu.edu/metro21/projects/reducing-congestion-and-emissions-with-an-airbnb-for-intelligent-curbs.html

7 https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

8 *Preparing for the Future of Artificial Intelligence.* Executive Office of the President, National Science and Technology Council Committee on Technology. October 2016.

9 https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf

10 *The National Artificial Intelligence Research and Development Strategic Plan.* National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee. October 2016.

11 https://www.govinfo.gov/content/pkg/FR-2017-01-12/pdf/2016-31059.pdf

12 https://mashable.com/article/lyft-self-driving-cars-las-vegas-50000-rides/?europe=true

13 https://www.theguardian.com/technology/2019/apr/19/ubers-self-driving-car-unit-valued-at-73bn-as-it-gears-up-for-ipo

14 https://newsroom.intel.com/editorials/krzanich-the-future-of-automated-driving/#gs.fxuhty

15 https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive and Assembly/Our Insights/Monetizing car data/Monetizing-car-data.ashx

16 Burkacky, Ondrej; Diechmann, Johnannes; Doll, Georg; Knochenhauer, Christian. *Rethinking Car Software and Electronics Architecture*. McKinsey Center for Future Mobility. February 2018.

17 Audi eTRON website, accessed November 15, 2019. https://www.e-tron.audi/en/well-connected-audi-connect-and-assist-systems-10678

18 Boagey, Rachel. "Ethernet: the fast track to the connected car," *Automotive World*. August 20, 2014. Accessed November 15, 2019. https://www.automotiveworld.com/articles/ethernet-fast-track-connected-car/

19 Nelson, Gabe. "Connected car's connector: Ethernet," *Automotive News*. February 23, 2015. Accessed November 15, 2019. https://www.autonews.com/article/20150223/OEM06/302239991/connected-car-s-connector-ethernet

20 Winning, Amy. "Number of automotive ECUs continues to rise," *eeNews*. May 15, 2019, accessed November 5, 2019. https://www.eenewsautomotive.com/news/number-automotive-ecus-continues-rise

21 Bauer, Lee. "Smart Vehicle Architecture: Key to the Future of Automotive Sustainability." Aptiv website. August 14, 2019. Accessed November 15, 2019. https://www.aptiv.com/media/article/smart-vehicle-architecture-key-to-the-future-of-automotive-sustainability

22 "Automotive Sensors Market Circling In On US $44.2 Billion by 2026," CSO. June 19, 2019. Accessed November 5, 2019. https://www.cso.com.au/mediareleases/34784/automotive-sensors-market-circling-in-on-us-442/

23 Walford, Lynn. "The Who, What, When, Where, Why, and How of Lidar," *Auto Futures*. February 11, 2019. Accessed November 15, 2019. https://www.autofutures.tv/2019/02/11/the-who-what-when-where-why-and-how-of-lidar/

24 Nelson, Gabe. "Connected car's connector: Ethernet," *Automotive News*. February 23, 2015. Accessed October 15, 2019. https://www.autonews.com/article/20150223/OEM06/302239991/connected-car-s-connector-ethernet

25 Nelson, Gabe. "Connected car's connector: Ethernet," *Automotive News*. February 23, 2015. Accessed October 15, 2019. https://www.autonews.com/article/20150223/OEM06/302239991/connected-car-s-connector-ethernet

26 Boagey, Rachel. "Ethernet: the fast track to the connected car," Automotive World. August 20, 2014. Accessed October 15, 2019. https://www.automotiveworld.com/articles/ethernet-fast-track-connected-car/

27 "Molex Unveils 10 Gbps Automotive Ethernet Network at CES 2018". *Molex*. Accesses October 15, 2019. https://experience.molex.com/molex-unveils-10-gbps-automotive-ethernet-network-ces-2018/

28 "Report Reveals that recalls Aren't Going Away Anytime Soon," *Recall Masters Press Release*, February 19, 2019. Accessed November 5, 2019. https://www.recallmasters.com/2018-recalls/

29 Barry, Keith. "Ford and GM say 2020 models will have OTA capability, but the convenience isn't without safety or security risks," *Consumer Reports*. April 20, 2018. Accessed November 6, 2019. https://www.consumerreports.org/automotive-technology/automakers-embrace-over-the-air-updates-can-we-trust-digital-car-repair/

30 Quain, John R. "With benefits — and risks — software updates are coming to the car," *Digital Trends*. October 29, 2018. Accessed November 5, 2019. https://www.digitaltrends.com/cars/over-the-air-software-updates-cars-pros-cons/

31 Williams, Brett. "Here's how every major automaker plans to go electric," *Mashable*. October 3, 2017. Accessed November 1, 2019. https://mashable.com/2017/10/03/electric-car-development-plans-ford-gm/

32 Douris, Constance. "The Bottom Line On Electric Cars: They're Cheaper To Own," *Forbes*. October 24, 2017. Accessed November 1, 2019. https://www.forbes.com/sites/constancedouris/2017/10/24/the-bottom-line-on-electric-cars-theyre-cheaper-to-own/#4349b1a110b6

33 Hawkins, Andrew J. "Electric car owners could choose which fake sounds their cars make under new proposal," *The Verge*. September 16, 2019. Accessed November 1, 2019. https://www.theverge.com/2019/9/16/20869035/electric-car-ev-fake-noise-nhtsa

34 Hardman, Scott. "'High-perforamnce, Fun-to-Drive' Electric Vehicles: ITS-Davis Study Reveals Surprising Consumer Motives." ITS UC Davis Institute of Transportation Studies, University of California, Davis. No publish date. Accessed November 1, 2019. https://its.ucdavis.edu/blog-post/high-performance-fun-to-drive-electric-vehicles-uc-davis-study-reveals-surprising-consumer-motives/

35 *Reducing Pollution with Electric Vehicles.* Office of Energy Efficiency & Renewable Energy. No publish date. Accessed November 1, 2019. https://www.energy.gov/eere/electricvehicles/reducing-pollution-electric-vehicles

36 Tonachel, Luke. "Study: Electric Vehicles Can Dramatically Reduce Carbon Pollution from Transportation, and Improve Air Quality." Natural Resources Defense Council. September 17, 2015. Accessed November 1, 2019. https://www.nrdc.org/experts/luke-tonachel/study-electric-vehicles-can-dramatically-reduce-carbon-pollution

37 Schwartz, Hart. "Americas Aging Vehicles Delay Rate of Fleet Turnover." *The FUSE*. January 23, 2018. Accessed November 1, 2019. http://energyfuse.org/americas-aging-vehicles-delay-rate-fleet-turnover/

38 Nikiforuk, Andrew. "The Big Shift Last Time: From Horse Dung to Car Smog," *The Tyee*. March 6, 2013. Accessed November 1, 2019. https://thetyee.ca/News/2013/03/06/Horse-Dung-Big-Shift/

39 Greimel, Hans. "Toyota amps up U.S. EV plans to join new 'surge'," *Automotive News*. June 10, 2019. Accessed November 1, 2019. https://www.autonews.com/sales/toyota-amps-us-ev-plans-join-new-surge

40 Carey, Nick and White, Joseph. "Ford plans $11 billion investment, 40 electrified vehicles by 2022." Reuters Business News. January 14, 2018. Accessed November 1, 2019. https://www.reuters.com/article/us-autoshow-detroit-ford-motor/ford-plans-11-billion-investment-40-electrified-vehicles-by-2022-idUSKBN1F30YZ

41 Lambert, Fred. "Renault, Nissan & Mitsubishi alliance will launch 12 new all-electric vehicles within the next 5 years," *Electrek*. September 15, 2017. Accessed November 1, 2019. https://electrek.co/2017/09/15/renault-nissan-mitsubishi-alliance-12-new-all-electric-vehicles/

42 Kane, Mark. "Volkswagen Starts Final Countdown To Phase Out Of Gas, Diesel," *InsideEVs*. December 5, 2018. Accessed November, 1, 2019. https://insideevs.com/news/341390/volkswagen-starts-final-countdown-to-phase-out-of-gas-diesel/

43 Riley, Charles. "Europe's switch to electric cars is accelerating. Honda is advancing its plans by 3 years." *CNN Business*. October 23, 2019. Accessed November 1, 2019. https://www.cnn.com/2019/10/23/cars/honda-electric-cars-europe/index.html

44 Petroff, Alanna. "These countries want to ditch gas and diesel cars," *CNN Business*. July 26, 2017. Accessed November 1, 2019. https://money.cnn.com/2017/07/26/autos/countries-that-are-banning-gas-cars-for-electric/index.html

45 "China targets 35 million vehicle sales by 2025, NEVs to make up one-fifth," *Reuters*. April 24, 2017. Accessed November 1, 2019. https://www.reuters.com/article/us-china-autos-electric/china-targets-35-million-vehicle-sales-by-2025-nevs-to-make-up-one-fifth-idUSKBN17R086

46 "British Columbia passes Zero-Emission Vehicles Act; 10% LDVs ZEV by 2025, 100% by 2040," *Green Car Congress*. June 3, 2019. Accessed November 1, 2019. https://www.greencarcongress.com/2019/06/20190603-bc.htm

47 Toth, Jacqueline. "For Widespread Adoption of Electric Vehicles, Many Roadblocks Ahead," *Morning Consult*. May 22, 2019. Accessed November 1, 2019. https://morningconsult.com/2019/05/22/for-widespread-adoption-of-electric-vehicles-many-roadblocks-ahead/

48 "National Household Travel Survey Daily Travel Quick Facts." Bureau of Transportation Statistics, United States Department of Transportation. Updated May 31, 2017. Accessed November 1, 2019. https://www.bts.gov/statistical-products/surveys/national-household-travel-survey-daily-travel-quick-facts

49 Charlton, Alistair. "The longest range electric cars of 2019: new EVs with the most charge," *Car Magazine*. September 27, 2019. Accessed November 1, 2019. https://www.carmagazine.co.uk/electric/longest-range-electric-cars-ev/

50 Coren, Michael J. "The median electric car in the US is getting cheaper," *Quartz*. August 26, 2019. Accessed November 1, 2019. https://qz.com/1695602/the-average-electric-vehicle-is-getting-cheaper-in-the-us/

51 Karr, Anthony. "Watch Electric Ford F-150 Tow More Than 1 Million Pounds," *Motor1*. July 23, 2019. Accessed November 1, 2019. https://www.motor1.com/news/361301/f150-electric-towing-million-pounds/

52 2019 F-150 Capability, Best-in-Class Capability for Work or Play. Ford Motor Corporation. Accessed November 1, 2019. https://www.ford.com/trucks/f150/2019/features/capability/

53 Perkins, Chris. "Rivian R1S and R1T: Everything We Know," *Road and Track*. October 24, 2019. Accessed November 1, 2019. https://www.roadandtrack.com/new-cars/future-cars/a29551028/2021-rivian-r1s-r1t-electric-trucks-details-rumors-photos/

54 "2021 Rivian R1T," *Car and Driver*. No publish date. Accessed November 1, 2019. https://www.caranddriver.com/rivian/r1t

55 McGlothlin, Mike. "Is the Electric Atlis XT a Thread to the Diesel Pickup's Dominance?" *DrivingLine*. May 10, 2019. Accessed November 1, 2019. https://www.drivingline.com/articles/is-the-electric-atlis-xt-a-threat-to-the-diesel-pickup-s-dominance/

56 "Which 13 electric SUVs are taking on Tesla's Model X?" *Business Insider*. October 12, 2018. Accessed November 1, 2019. https://www.scmp.com/magazines/style/tech-design/article/2168115/which-13-electric-suvs-are-taking-teslas-model-x

57 Lambert, Fred. "Mercedes-Benz unveils EQV all-electric minivan with almost 250 miles of range," *Electrek*. March 5, 2019. Accessed November 1, 2019. https://electrek.co/2019/03/05/mercedes-benz-eqv-electric-minivan/

58 Hanley, Steve. "Chrysler Schedules Portal Electric Minivan For 2020 Production," *CleanTechnica*. September 18, 2018. Accessed November 1, 2019. https://cleantechnica.com/2018/09/18/chrysler-schedules-portal-electric-minivan-for-production/

59 3 Revolutions Future Mobility Program. University of California, Davis. Accessed November 1, 2019. https://3rev.ucdavis.edu/

60 Millennial's Car Rental Issues & Alternatives," Debt.org. June 30, 2017. Accessed November 1, 2019. https://www.debt.org/blog/millennials-car-rental-issues-alternatives/

61 Fluid Market. "Fluid Market Launches Truck Sharing Marketplace." Denver, CO. February 15, 2018. Accessed November 1, 2019. https://www.prnewswire.com/news-releases/fluid-market-launches-truck-sharing-marketplace-300599269.html

62 Jenn, Alan. "Emissions Benefits of Electric Vehicles in Uber and Lyft Services." National Center for Sustainable Transportation. ITS UC Davis Institute of Transportation Studies. University of California, Davis. August 2019. Accessed November 1, 2019. https://escholarship.org/uc/item/15s1h1kn

63 "National EV Market Growth Accelerated in 2018." National Overview of TNC Electrification, EV Shared Mobility. Accessed November 1, 2019. http://evsharedmobility.org/national-overview-of-tnc-electrification/

64 Dawid, Irvin. "Charger Rage Hits Electric Vehicle Country in California," *Planetizen*. October 12, 2015. Accessed November 1, 2019. https://www.planetizen.com/node/81557/charger-rage-hits-electric-vehicle-country-california

65 https://www.isecom.org/OSSTMM.3.pdf

66 Harkins, Malcolm. *The Rise of the Cyber industrial Complex and Expense in Death*. Institute for Critical Infrastructure Technology. July 2019.

67 Spaniel, Drew and Roy, Rob. *Software Security is National Security*. Institute for Critical Infrastructure Technology. April 2019.

68 Leveson, Nancy. "A New Accident Model for Engineering Safer Systems," *Safety Science*. April 2004, pp. 237-270.

69 Ibid.

70 Kurd, Z.; Kelly, T.; AND J. Austin. "Developing artificial neural networks for safety critical systems," Neural Computing and Applications, 16 (2007), pp. 11–19.

71 McDermid, J.; Daffey, K. Safety of Artificial Intelligence and its role in Autonomy: A MaritimePerspective, in 2018 Safety Critical Systems Symposium, SSS '18, York, UK, 2018, Safety-Critical Systems Club.

72 Schroeder, Bianca; Pinheiro, Eduardo; Weber, Wolf-Dietrich. "DRAM Errors in the Wild: a Large-scale Field Study," in Proceedings of the eleventh international joint conference on Measurement and modeling of computer systems, SIGMETRICS '09, New York, NY, USA, 2009, ACM, pp. 193–204.

73 Kim, Yoongu; Daly, Ross; Kim, Jeremie; Fallin, Chris; Lee, Ji-Hye; Lee, Donghyuk; Wilkerson, Chris; Lai, Konrad; and Mutlu, Onur. "Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors," in ACM/IEEE 41st International Symposium on Computer Architecture, ISCA 2014, Minneapolis, MN, USA, June 14-18, 2014, pp. 361–372.

74 Koopman, Philip. "The Heavy Tail Safety Ceiling", in Automated and Connected Vehicle Systems Testing Symposium, Greenville, South Carolina, USA, 2018.

75 Zittrain, Jonathan, *Intellectual Debt: With Great Power Comes Great Ignorance*, 2019.

76 Kim, Yoongu; Daly, Ross; Kim, Jeremie; Fallin, Chris; Lee, Ji-Hye; Lee, Donghyuk; Wilkerson, Chris; Lai, Konrad; and Mutlu, Onur. "Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors," in ACM/IEEE 41st International Symposium on Computer Architecture, ISCA 2014, Minneapolis, MN, USA, June 14-18, 2014, pp. 361–372.

77 Szegedy, Christian; Aremba, Wojciech; Sutskever, Ilya; Bruna, Joan; Erhan, Dumitru; Goodfellow, Ian; and Fergus, Rob. *Intriguing properties of neural networks*." 2013.

78 McCabe, T. J. "A complexity measure," IEEE Transactions on Software Engineering. Volume SE-2, Issue 4. December 1976, pp. 308–320.

79 The prefix "ISO/PAS" indicates that this is not a standard, but rather a "publicly available specification".

80 Koopman, Philip. "The Heavy Tail Safety Ceiling", in Automated and Connected Vehicle Systems Testing Symposium, Greenville, South Carolina, USA, 2018.

81 Leveson, Nancy. Engineering a Safer World. 2011. The MIT Press. Cambridge, Massachusetts and London, England. Leveson, Nancy; Daouk, Mirna; Dulac, Nicholas; and Marais, Karen. "Applying STAM in Accident Analysis," Massachusetts Institue of Technology. 2003.

82 Sharma, S.; Flores, A.; Moreno, C.; Hobbs, C.; Stafford, J.; Lamichhane, K.; Fischmeister, S.; and Khan, W. "Lessons-l;earned from Applying STAMP Safety and Security Analysis on AEB for L4 Autonomous Driving." Partnership for Systems Approaches to Safety and Security (PSASS), 2019.

83 Lauterbach, Anastassia; Bonime-Blanc, Andrea. *The Artificial Intelligence Imperative: A Practical Roadmap for Business*. 2018, p. 68.

84 Krakovna, Viktoriya. *Building Interpretable Models: From Bayesian Networks to Neural Networks*. Ph.D Thesis, Harvard University, Cambridge, Massachusetts. September 2016.

85 Leveson, Nancy. *Engineering a Safer World*. 2011. The MIT Press. Cambridge, Massachusetts and London, England.

86 Hobbs, Chris. *Die Verbesserung des Sicherheitsnachweises durch Induktion: Kann ein Denkbegriff aus dem 16. Jahrhundert nu¨tzlich sein?* in Proceedings of ESE Kongress 2018.

87 https://www.nature.com/articles/s41586-018-0637-6

88 https://pages.nist.gov/800-63-3/sp800-63b.html

89 https://get.clt.re/age-and-experience-on-risk-and-security/

90 Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices

91 http://blackberry.qnx.com/en/news/webinars#!/webinar/22

92 https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/

93 *Upstream Security Global Automotive Cybersecurity Report 2019: Research into Smart Mobility Cyber Attack Trends.* Upstream.auto. 2019.