OK

By Jeremy Spaulding, Emma Grossman, Aidan Reilly Giunta
Corresponding Author: Jeremy Spaulding, AutoNebula Group, jspaulding@autonebula.com

Today's cars are capable of sharing information with each other and have been for a number of years now. Some cars connect via cellular signals through telematics services, e.g. OnStar, serve as mobile hotspots for Wi-Fi, and some are even introducing serve as mobile

safety Vehicle Intrusion Protected Applications (EVITA). These three institutions have been expanding their models while working together, so that all these threat models can be designed and implemented swiftly to protect the future of the automotive industry. The University of Michigan goes on to say that "The existing models by the NHTSA and EVITA are good, comprehensive examinations that look at automotive applications and their vulnerabilities but omit considerations about specific sources and actors behind security threats, their motivations, and how they weigh the risks involved in considering an attack".[11]

As technology becomes more advanced and more autonomous, the cybersecurity that is needed to keep it secure becomes more difficult and intricate. When a new component is implemented into the system, all the other systems' security features need to be reevaluated to make sure that the newly implemented system works with its current security. If it does not, then the entire security system needs to be redesigned to make sure that all the systems are continually kept secure from outside intrusions.

The first such implemented autonomous vehicle that was sold to the general public was Tesla's 2014 Model S. The Model S was equipped with Tesla's "Hardware 1" autopilot system. That first generation of autonomy only included the feature for the vehicle to have some semi-autonomous driving and self-parking. In 2015, Tesla released "Autopilot version 7.0" which included the full autonomy while driving down the highway, but was quickly replaced by version 7.1, to remove some features that would encourage drivers to not pay attention to the road because of said autonomy. Version 7.1 also added the "summon" feature, which would allow the car to self-drive to your location with the press of a button on your key fob.

Vehicles using Tesla's Autopilot system have been involved in numerous incidents, some that were fatal to the user. Tesla has attempted to remedy these imperfections in the system and have installed fail-safes, such as insisting that the driver of the car must touch the steering wheel every couple of minutes to tell the system that they are still present and paying attention to the road while the car is in Autopilot.

Technology like this requires a lot of trial and error, but whether or not it should be released until those errors are sorted out remains a critical question that will remain at the center of our societal dialogue about these emerging technologies.

Designing integrated systems, in part via industrial internet of things (IIoT), involves interoperability which in turn requires both a degree of standardization and that the entire infrastructure is established in a common and interchangeable way. In the Tesla example, this could be one of the biggest hurdles. The infrastructure in the United States is still accepting this new form of transportation and the roadways need development. PricewaterhouseCoopers (PwC) emphasizes that the world has "megatrends" that are affecting the way our infrastructure is going to need to be reshaped.[12] These megatrends include demographic shifts, economic power shifts, technological breakthroughs, accelerating urbanization, and climate change. These megatrends then combine with industry-changing technological breakthroughs to establish what types of mobility infrastructure will need to be developed. PwC articulates that the five infrastructure changes needed are:

1) Small,

These five changes to our infrastructure will allow for a more prosperous growth of the autonomous vehicle industry.

A CSO article written in 2017 by Lohrmann, states that internet of things (IoT) technology is quickly developing and has become a hot topic, but cybersecurity and the known vulnerabilities associated with IOT technologies do not receive the attention that they should. One such example of IoT device hacking is what is known as a Distributed Denial of Service (DDoS) attack, which in certain instances has caused multiple utilities to be shutdown.[13] The Harvard Business Review stated:

> "Simple computer bugs can also cause significant glitches in control systems, leading to major technical problems for cities. Once hackers invade smart city control systems, they can send manipulated date to severs to exploit and crash entire data centers."[14]

As a whole, smart city infrastructure requires a lot more development before it can provide the general public with confidence in its abilities.

Nick Ismail with Information Age states that with the current influx of people moving into urban areas, the adjustment to smart city infrastructure could end up saving five trillion dollars by 2022.[15] He states

In nearly every sector, antiquated and static regulatory frameworks are being challenged by new and emerging technologies, and the automotive industry is no exception. Advancements in autonomous vehicle technology have presented a major challenge when it comes to the U.S. regulatory framework. Technological developments are progressing at a much faster rate than policymakers can keep up with. Current regulations are based, with good reason, on a tradition of motor vehicles that have been manually operated by humans. Yet even the technologies integrated into many vehicles that are on our roads today already assume certain responsibilities in the operation of themselves, stretching the efficacy of existing regulatory mechanisms. The eventual elimination of humans as chief operators all together will only exacerbate this tension. These unresolved issues have left local, state, and federal policymakers struggling to keep pace.

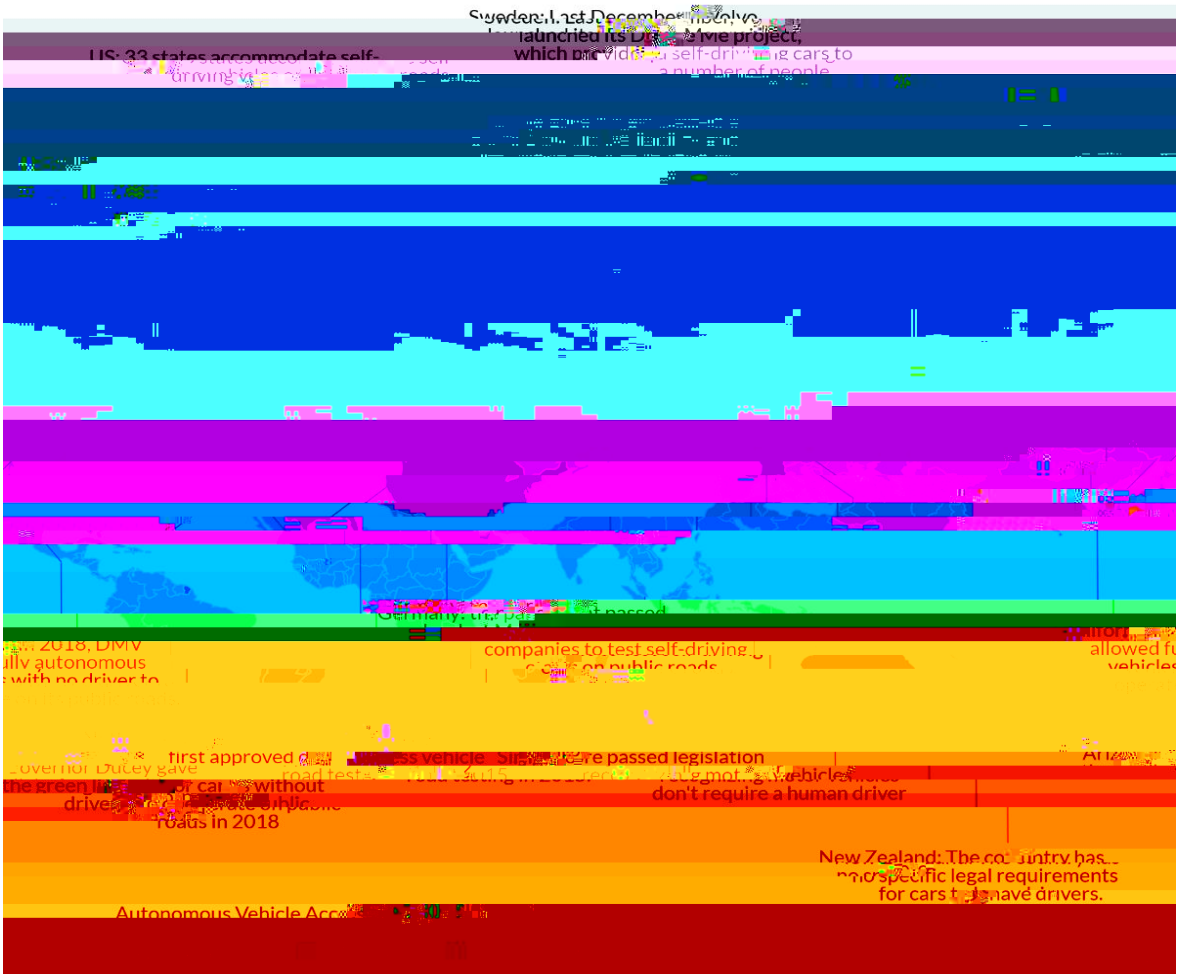


Figure 1: Major regions accommodating deployment and testing of autonomous vehicle technologies on public roads.

autonomous taxi service and have plans to implement the service fully by the end of 2018.[23] With different countries progressing at different rates, those that do not begin to seriously focus on finding solutions and driving innovation will find themselves falling behind.

Finding the balance between competition and collaboration

hubs will increase as more people seek to live there, potentially causing a housing shortage in these areas, as demand will outstrip available supply.

Furthermore, according to statistics presented by Razin, private automobiles spend just 5% of their time actually in use, while these vehicles stayed parked during the remaining time. The need for parking has resulted in around 500 million parking spaces in this country, which is commercial real estate. In an age

So no, we are not ready yet for a fully-autonomous future, but we are not far off, and we are getting closer every day. The relentless forward march of technology means that soon the capability for autonomy will arrive. We must work to ensure that we are prepared on all other fronts for that day.

Keeping an open mind and thinking in the long-term is just as important as looking at the short-term. For example, safety has been a major concern with the multitude of accidents and failures that have been associated with autonomous vehicle testing and development. All of the concern is understandable, but it is also important that we do not shy away from continuing to make improvements and find solutions to these problems.

Education is a crucial component of any societal movement. Fear of the unknown is another natural reaction that we have as humans. It is important that policymakers and the public are kept up to date with enough transparency to understand what is going on in the industry. Knowledge is power and an educated public and government will be much more understanding and willing to find ways to overcome the multitude of hurdles that accompany the changing landscape.

Angerholzer, M., III, Mahaffee, D., Vale, M., Kitfield, J., & Renner, H. (2017, March). The Autonomous Vehicle Revolution (Rep.). Retrieved July 11, 2018, from CSPC website: https://www.thepresidency.org/sites/default/files/pdf/The Autonomous Vehicle Revolution—Fostering Innovation with Smart Regulation.compressed.pdf

Alert (ICS-ALERT-17-209-01). (2017, July 28). Retrieved July 10, 2018, from https://ics-cert.us-

Weimerskirch, A., & Dominic, D. (2018). Assessing Risk: Identifying and Analyzing CybersecurityThreats to Automated Vehicles. University of Michigan,1-10. Retrieved July 10, 2018, from https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf

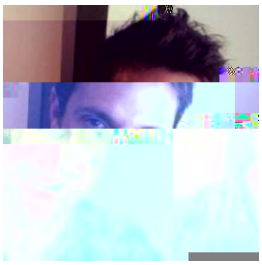
The opinions expressed in this article are those solely of the author.

Corresponding Author

JEREMY SPAULDING
jspaulding@autonebula.com

Founder and President, JMS Innovation & Strategy

Senior Vice President, Technology, AutoNebula Group



Spaulding has a master's degree in Industrial & Systems Engineering/Human Factors from Virginia Tech and over 15 years of experience in Human Factors Research, HMI development, usability analysis and user experience development for major corporations in the lighting, automotive, software, and healthcare industries. He is an active Advisory Board Member of the Woodrow Wilson Center's Science and Technology Innovation Center (STIP) in Washington DC.

The Wilson Center
Web: wilsoncenter.org
Facebook: WoodrowWilsonCenter
Twitter: @TheWilsonCenter
Phone: 202.691.4000

The Digital Futures Project
Web: wilsoncenter.org/program/digital-futuresproject
Email: digitalfutures@wilsoncenter.org
Facebook: WilsonCenterDFP
Twitter: @WilsonCenterDFP
Phone: 202.691.4002

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027