PUBLISHED JUNE 2022

Autonomous Vehicles and Cyber Risk

CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

Autonomous Vehicles and Cyber Risk

Published June 2022

Summary

The line between cyber and auto insurance is blurring as sophisticated and often internet-connected autonomous vehicles (AV) become more prevalent. This section discusses the growth of AVs, their benefits, and their cyber risks, in addition to legislation and current regulations overseeing cyber insurance.

Introduction

According to one industry projection, the global market for automated vehicles is expected to grow[1] from 0.1% of vehicle registration share in 2021 to 12% or approximately 101 million units in 2030.

The global autonomous commercial vehicle market is expected to grow from $5.59 billion in 2020 to $7.07 billion in 2021 at a compound annual growth rate (CAGR) of 26.5%. The market is expected to reach $13.41 billion in 2025 at a CAGR of 17%.[2]

Major players in the autonomous commercial vehicle market include Volkswagen, Daimler AG, Tesla, Denso, Continental, Waymo, BMW AG, Isuzu Motors Limited, General Motors, and AB Volvo.

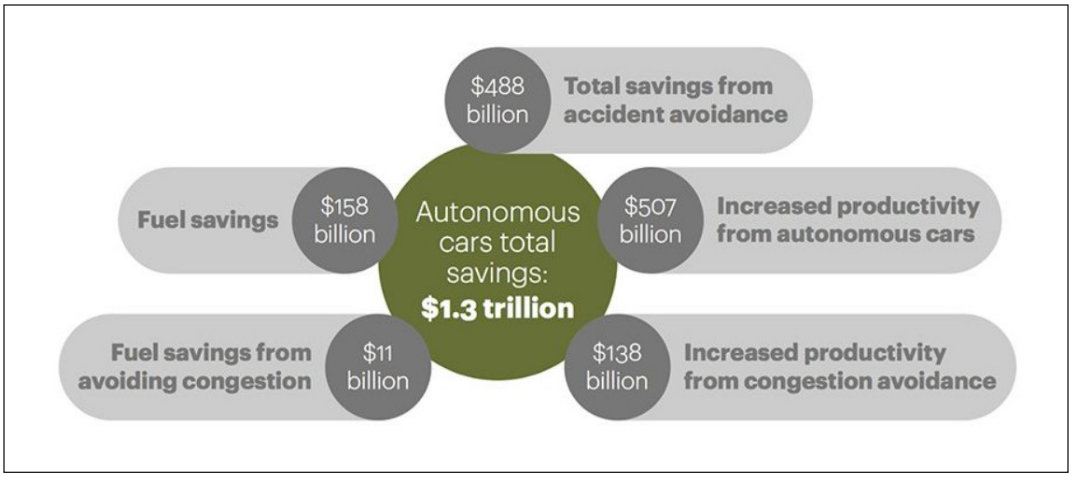
Benefits of Autonomous Vehicles

One industry survey, *The Road to Autonomous Vehicles—2018*,[3] found that 7 in 10 Americans (70 percent) believe autonomous vehicles will routinely navigate the nation's streets and highways within 15 years.

1 "Projected autonomous vehicle registration share worldwide between 2021 and 2030"; Statista; Aug. 5, 2021.
2 "Autonomous Commercial Vehicle Global Market Report 2021: Breakdown by Driver Assistance, Partial Automation, Conditional Automation, High Automation, Full Automation"; ResearchAndMarkets.com; Aug. 26, 2021.
3 "Americans Expect Self-Driving Vehicles to be Commonplace within 15 Years"; *ITS Digest*; June 4, 2018.

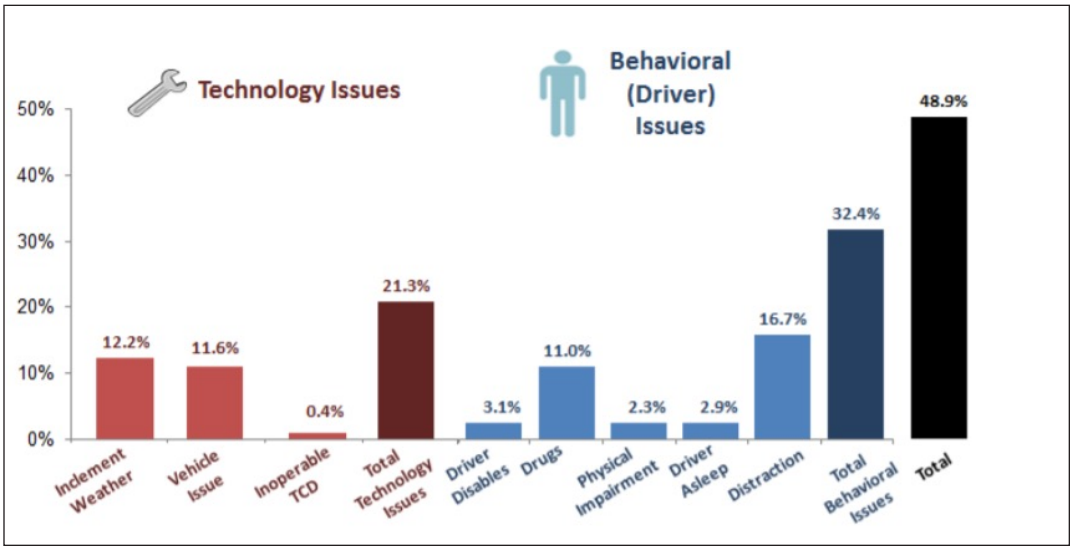
According to another industry study,[4] the growth of AVs could represent a $1.3 trillion boost to the U.S. economy. For comparison, the U.S. nominal GDP in 2021 was $20.5 trillion.[5]

Figure 11



In 2018, the Casualty Actuarial Society's Automated Vehicles Task Force published a paper[6] that presented an illustration of driver behavior as being the largest contributor to accidents, followed by technology issues (when extrapolated):

Figure 12



Based on this information, by eliminating the driver from the equation, autonomous cars can be expected to be safer, as the increase in potential technology issues is far outweighed by the removal of the behavioral issues.

4 "US autonomous vehicle market could hit $560 billion by 2035"; Consulting.us.; July 25, 2019.
5 "GDP Ranked by Country 2022"; World Population Review; 2022.
6 Automated Vehicles and the Insurance Industry; Casualty Actuarial Society; 2018.

This would in turn be expected to shift the liability from individual drivers to the vehicle manufacturers. The same paper calculates the insurance premium impact of this shift with assumptions, such as:

- Every vehicle is fully autonomous.
- Every vehicle is fully owned by the manufacturer.
- $1 million policy limits.
- Frequency remains the same.

The paper projects that the average premium would double or triple, caused mostly by dramatically increasing the coverage of each vehicle. However, the frequency is expected to decrease. Under different scenarios, the paper calculates a frequency reduction slightly above 50% is going to cause average premiums to decrease instead.

Some expect the biggest benefit of AV for long-haul trucks is doubling the asset utilization by eliminating the need for mandated truck stops. A second benefit is mitigating the shortage of drivers available, which has historically been the highest-cost line item in the industry.[7]

Cyber Risks in Autonomous Vehicles

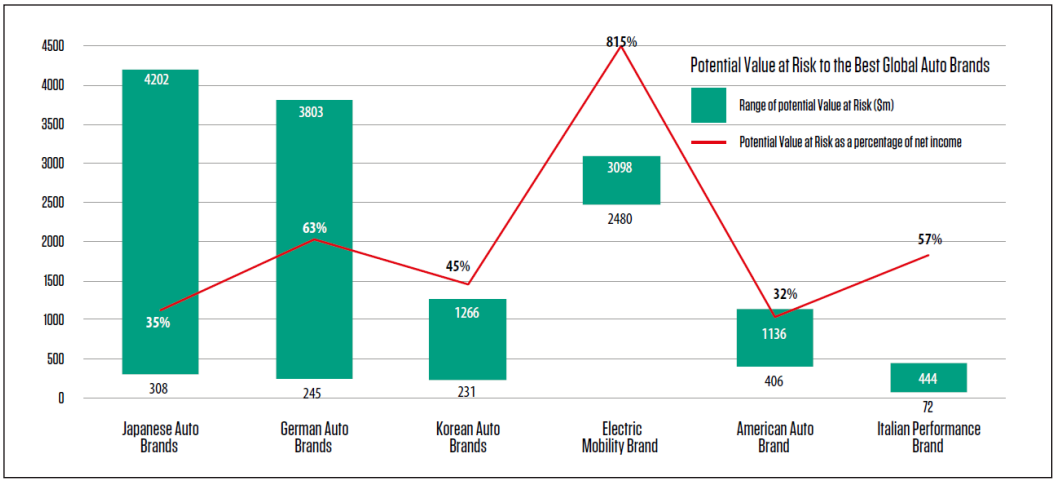
The integration of motor vehicles with electronic systems slowly turns them into connected devices. Several vehicle manufacturers even provide over-the-air (OTA) updates, while others are equipped with Wi-Fi for their passengers. Turning cars into connected devices adds new cyber risks including exposure, theft, and tampering.

Therefore, the level of security required to protect these vehicles extend far beyond the entry points of the vehicle itself, both wired and wireless. To accomplish this, OTA updates need to use the appropriate encryption methods; data warehouses used by the manufacturers to receive and transmit vehicle data need to be safeguarded; and standards need to be created that articulate best practices in the industry.

7 "Autonomous commercial vehicles: ready for the road?"; Kearney.

How about the level of cyber risk faced by the auto industry? A 2021 industry report produced by a digital services consulting firm[8] quantifies the value at risk in this way:

Figure 13



Invisible Tech—Real Impact: The Industry View

Some recent cyber-attacks illustrate the potential of future impacts:

- Two researchers have displayed how a zero-click exploit[9] could be used to hack Tesla—and possibly other cars—remotely, using a drone. The researchers showed how to take full control of the infotainment system (although not the drive control itself). While Tesla has patched this vulnerability, the vulnerable component is widely used in the auto industry, which means that other cars could be vulnerable.

- One of Honda Motor Company's internal servers was attacked[10] by a case of Ekans ransomware in 2020, affecting its production, sales, and development activities. Ekans uses RSA[11] encryption to lock up impacted machines and will go on a "process killing rampage, terminating any system that could become a barrier to the malware's activities and deleting shadow copies in the process to make it more difficult to recover files."[12]

8 *Invisible Tech—Real Impact*; Infosys; 2021.
9 "Tesla Car Hacked Remotely From Drone via Zero-Click Exploit"; *SecurityWeek*; May 3, 2021.
10 "Honda's global operations hit by cyber-attack"; BBC News; June 9, 2020.
11 Rivest, Shamir and Adleman (RSA) algorithm, a public key encryption technique.
12 "This is how EKANS ransomware is targeting industrial control systems"; *ZDNet*; July 2, 2020.

- During a test drive in 2019 using Tesla's Navigate on Autopilot feature, a staged attack[13] caused a car to suddenly slow down and unexpectedly veer off the main road. Researchers "found that 'spoofing' attacks on the Tesla GNSS receiver could easily be carried out wirelessly and remotely, exploiting security vulnerabilities in mission-critical telematics, sensor fusion, and navigation capabilities."[14]

- A hacker named "EvanConnect" developed a device in 2020 that can break into any luxury car that uses a wireless key fob system. It is being sold for $12,000. One security expert said that the "keyless repeater technology is commonly known in the field."[15]

Clearly, as vehicle systems become increasingly interconnected, more potential cyber exposures will exist, and therefore stronger cybersecurity measures will be necessary for the manufacturers of autonomous vehicles. It is equally important for the vehicle owners to ensure software updates are done on time.

Federal and State Legislative and Regulatory Outlook

There is currently no comprehensive federal or state-level regulatory structure for AV vehicles in the United States.[16] Traditionally, both federal and state agencies work together to regulate the safety of passenger vehicles.

A congressional bill H.R. 3711,[17] also known as the Self Drive Act, would have prescribed the safety standards for highly automated vehicles. Two attempts to pass the bill in 2017 and 2020 both failed due to concerns about the language. However, key federal lawmakers have recently noted they intend to enact legislation to create federal safety and security standards for autonomous vehicles.[18]

In *Automated Driving Systems: A Vision for Safety*,[19] the National Highway Traffic Safety Administration (NHTSA) laid out voluntary guidance, technical assistance to states with respect to federal and state roles, best practices for consideration in legislating in this area, as well as "best practices for state highway safety officials."

13 "How Hackers Can Take Over Your Car's GPS"; *Claims Journal*; June 19, 2019.
14 "Tesla Model S and Model 3 vulnerable to GNSS spoofing attacks"; GPS World; June 28, 2019.
15 "Hacker creates new device that can unlock any luxury car"; The Economic Times; Feb. 17, 2020.
16 *Autonomous Vehicles: Legal and Regulatory Developments in the United States*; Jones Day; July 2021.
17 *H.R.3711—SELF DRIVE Act*; Congress.gov; June 4, 2021.
18 "Congress makes renewed push on self-driving cars bill"; *The Hill*; Feb. 17, 2021.
19 *Automated Driving Systems 2.0: A Vision for Safety*; U.S. Department of Transportation; September 2017.

In June 2020, the Department of Transportation (DOT) launched the AV TEST initiative, a cooperative effort between the DOT, 52 companies, state governments, and associations with the purpose of "coordinating and sharing information in a standard way."

There are six levels of self-driving according to a standard setter:[20]

1. Level 0—No Driving Automation
2. Level 1—Driver Assistance
3. Level 2—Partial Driving Automation
4. Level 3—Conditional Driving Automation
5. Level 4—High Driving Automation
6. Level 5—Full Driving Automation

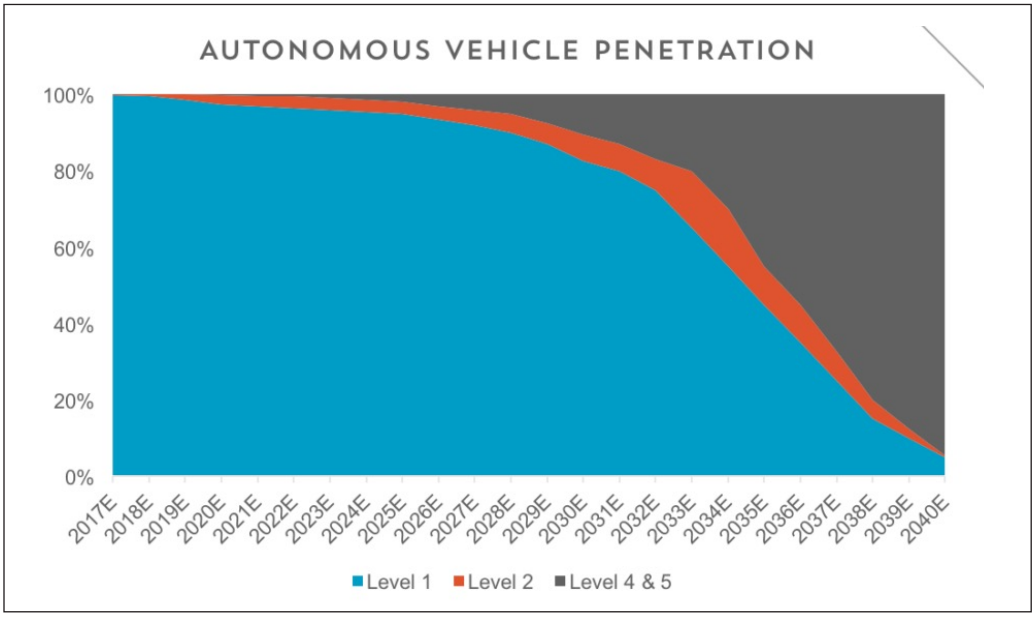
In 2020, NHTSA published an advance notice of proposed rulemaking to "obtain public comments on the development of a framework for Automated Driving Systems (ADS) safety."[21] The framework's intent is to "objectively define, assess, and manage the safety of ADS performance while ensuring the needed flexibility to make further innovation." It had a comment period that ended in April 2021.[22]

In November 2020, the FCC split the 5.9 GHz band between dedicated ranges for Wi-Fi and C-V2X (Cellular-Vehicle-to-Everything) in order to "enhance automobile safety."

20 *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*; SAE International; April 2021.
21 *Framework for Automated Driving System Safety*; National Highway Traffic Safety Administration; Nov. 19, 2020.
22 "Framework for Automated Driving System Safety; Extension of Comment Period"; National Highway Traffic Safety Administration; Jan. 29, 2021.

One industry source[23] projects the following market penetration by self-driving level in the next 20 years:

Figure 14



Source: Loup Ventures

According to the National Conference of State Legislatures,[24] as of 2020, 29 states had enacted laws related to autonomous vehicles. However, as of 2021, 37 states and D.C. have some kind of AV-related regulation.[25]

More could be done on this front, especially when we consider other countries: The United Kingdom (UK)[26] and Germany,[27] for example, have enacted laws to address liability issues.

In June 2020, 53 countries adopted a United Nations regulation[28] for jurisdictions that adhere to it that would require national regulators to guarantee vehicles are adequately protected against potential cyber security attacks. The regulation also would require manufacturers to ensure that suppliers include cyber security protection such as forensic technology able to decipher cyber-attacks.

While the U.S. participated in discussions in the development of the regulatory agreement, it did not vote and has not implemented the regulation. However, those that sell vehicles in jurisdictions where the cyber security regulation has been implemented must comply.

23 *Auto Outlook 2040: The Rise of Fully Autonomous Vehicles*; Loup Ventures; Sept. 6, 2017.
24 "Autonomous Vehicles State Bill Tracking Database"; National Conference of State Legislatures; March 16. 2022.
25 *Autonomous Vehicles: Legal and Regulatory Developments in the United States*; Op. cit.
26 *Automated and Electric Vehicles Act 2018*; Legislation.gov.uk.; 2018.
27 "Gesetz zum autonomen Fahren tritt in Kraft"; German Federal Ministry for Digital and Transport; July 27, 2021.
28 "U.N. Announces New Cyber Security Regulation for Connected Vehicles"; IEEE.org.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**