Autonomous Vehicles: Risk Management Issues and Concerns

March 2017 • Lockton Companies

Do you drive your car or does your car drive you? The answer to that question may change someday soon. The automotive industry is looking to find solutions that will lessen the impact of human error behind the wheel. They are designing cars that offer an ever-increasing amount of driving support with the intent to relinquish control to the vehicle.

Industry experts believe the automation of vehicles will reduce the number and severity of auto accidents, which has the potential to save thousands of lives and reduce the overall cost of vehicle ownership. As the world shifts its view of driving, a number of new risk management challenges may arise.

This paper will explore the insurance industry's concerns about the rising popularity of autonomous vehicles, specifically focusing on cyber security, shifts in liability exposures, and the effect these concerns will have on underwriting commercial auto policies.

AUTHOR

KATHRYN SERGEANT, CPCU, ARM, AINS
816.960.9976
ksergeant@lockton.com

LOCKTON®

WHAT IS AN AUTONOMOUS VEHICLE?

An autonomous vehicle is one that can operate under its own power. The National Highway Traffic Safety Administration developed five levels of autonomy for vehicles in 2013.[1]

LEVEL 0

No automation

This is the most common type of vehicle. Drivers are in control of all operations of the car. They may have automated warning systems, such as blind spot monitoring, forward collision, or lane departure warnings.

LEVEL 1

Function-specific automation

The Level 1 vehicle has one or more automated features, such as stability control or braking automation, with a goal of avoiding or lessening the impact of collisions. Despite these features, the driver is still in control. If the car has more than one automated feature, they work independently of one another.

LEVEL 2

Combined function automation

A Level 2 vehicle has two or more primary control functions that are designed to work in unison to relieve the driver of control. For example, the vehicle may have adaptive cruise control and lane-centering working together to keep it moving along the road while allowing the driver to relinquish control of steering and speed. The driver must be alert and available to take back the control at any moment.

LEVEL 3

Limited self-driving automation

Very little monitoring by the driver is required when operating a Level 3 vehicle. The vehicle has full control of all safety-critical functions. If a hazardous condition arises, the driver will receive a warning so he or she can retake control.

LEVEL 4

Full self-driving automation

A Level 4 vehicle is a true self-driving car. Once the driver provides destination or navigation input, the vehicle controls all driving and roadway monitoring functions.

Most vehicles on the road today fall within Levels 1 through 3. Companies like Google and Tesla Motors are working on technology to reach Level 4. It seems that fully autonomous, or self-driving, vehicles may not emerge as standard until 2050, providing ample time for determining an effective risk management approach.[2]

WHAT COULD GO WRONG?

No new technology comes without its drawbacks. As these autonomous vehicles are released into the market, what could go wrong? Several factors will need to be considered: cyber security, the shift in liability, and changes in underwriting to keep current with technology trends.

New Cyber Security Risks

It Comes Down to Control

The link between cyber security and cars is a new concept, and it's one that should not be underestimated. Here is an illustration. In July 2015, two hackers, Charlie Miller and Chris Valasek, developed a tool to hijack the controls of a Jeep Grand Cherokee while the driver, senior writer for *WIRED*, Andy Greenberg, was at the wheel in St. Louis. Andy did not know what exactly would happen during the experiment. He was surprised when his vehicle began blasting cold air, his radio station was switched, the windshield wipers turned on, and the transmission was cut while he was traveling at 70 mph down the highway. The hackers were able to take control of Andy's vehicle through the Jeep's entertainment system. Fortunately for Andy, he knew who was behind this attack and was aware it was coming. The hackers conducted this experiment as part of a grant funded by the Defense Advanced Research Projects Agency (DARPA). It is part of an effort to understand the vulnerability of vehicle systems to cyber attacks. Their findings indicated that more than 400,000 vehicles on the road today could be susceptible to cyber attacks.[3]

Mass auto cyber attacks are possible when systems are easily accessible for hackers. If a cyber attacker discovers a weakness in a certain vehicle type or a company's electronic system, it would be possible to disable large numbers of vehicles. Manufactures should be aware of any weaknesses in coding that may allow an outside party to access the system.

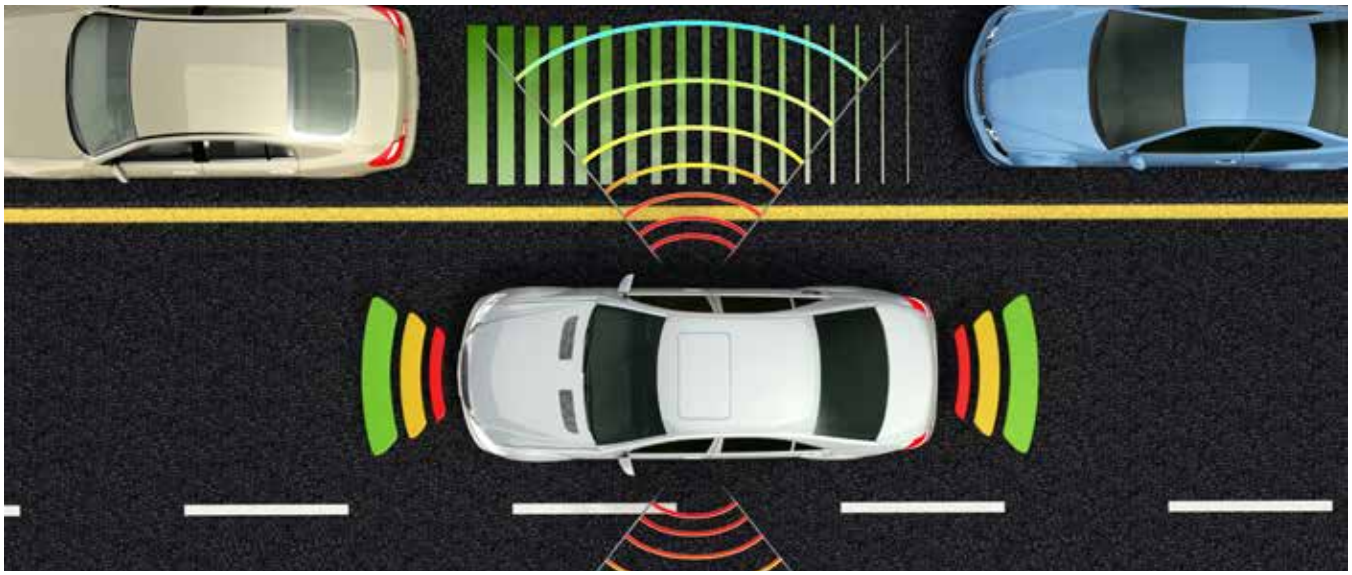
Proper security will deter cyber criminals from accessing individual autos to hold them for ransom. According to the *WIRED* article, while performing the hijack of the Jeep Grand Cherokee in St. Louis, the hackers were able to view hundreds of similar vehicles in other parts of the country. It would have been simple for them to access any of these other cars and disable the engine or control the entertainment system. The concern is that a hacker with criminal intent could disable an individual vehicle or a fleet of vehicles and hold them for ransom. The user would need to pay the hacker to regain the ability to control the auto.

The Necessary Evolution of Roads

Cyber security may also be a concern with new roadway technology that enables the operation of Level 3 and Level 4 vehicles. Self-driving cars require "smart roads" for operation. That means cameras and sensors are built into roadways and street signs. Sensors use radar and LiDAR (light detection and ranging) to communicate with the vehicles.

Some local governments are looking to invest in smart infrastructure that will allow communication between roads and the vehicles traveling on them. For example, Columbus, Ohio, recently won $65 million in grants to become the first US city to integrate self-driving cars, connected vehicles, and smart sensors. Atlanta, Georgia, has built a fiber and electrical network in its downtown corridor to support roadside sensors and cameras for driverless cars with hopes that technology companies will develop and test their products in the city.[4]

These "smart city" designs involve extensive communication networks that could be vulnerable to cyber attack. An interruption in these interconnected systems could cause significant damage. Because it's so new, this technology has not yet been put through its paces with security vulnerability testing. As cities begin to replace old infrastructure with new, the evaluation and monitoring of potential cyber security concerns will be crucial.



A Shift in Liability

Who Is Responsible?

The focus of auto insurance has been on the owner's liability. The current version of the commercial auto insurance form (ISO CA 00 01 10 13) specifically covers an insured's legal obligation for damages because of "bodily injury" or "property damage" caused by an accident that was the result of ownership, use, or maintenance of a vehicle. If the owner is distracted, under the influence, or fails to properly maintain the vehicle and causes an accident, insurance will cover the damages to the injured third party. But what happens when the vehicle is self-driving? The owner or driver either has limited or no control over circumstances that may lead to an accident.

The law may look to manufacturers to cover all or a portion of the liability, depending on the level of autonomy. Auto manufacturers may experience expanded liability and product risks as autonomous vehicles are introduced. The focus of accidents will be on what went wrong with the navigation, electronics, and the automated parts, rather than driver error. Responsibility for breakdowns or recalls may go to the manufacturer.

An Issue of Control: An Illustration

We can review the circumstances in the July 2016 Tesla Model S accident as one example of the type of system error that could occur. In 2015, Tesla released an autopilot mode in the Model S.[4] The following year, a driver of a Model S was operating it in autopilot mode, which means the car was autonomously braking, steering, and lane switching. The car collided with a tractor-trailer that was making a turn. The autopilot sensors failed to recognize the difference between the truck and bright sky, causing the collision.[5]

This incident resulted in the driver's death, the first fatality from a self-driving vehicle. The driver was not controlling the vehicle when the accident occurred, so it might seem logical to assume that the autopilot system and its manufacturer were at fault. But an investigation

by the National Highway Traffic Safety Administration found no defects in the Model S autopilot system. An NHTSA investigator noted that some situations are beyond the capabilities of the autopilot system, so "autopilot requires full driver engagement at all times." The investigation found that the driver might not have been paying attention to the road.[6]

Tesla still may have some responsibility in this accident, even though the technology did not fail. It is unknown whether Tesla properly informed the owner of the limits of the autopilot features. Auto manufacturers that are researching and developing autonomous technologies, like Google, Mercedes, and Volvo, have pledged to accept responsibility for accidents caused by malfunctions of the technology in their vehicles.[7] It is not clear, however, if they plan to absorb all of the risks associated with recalled or failed autonomous technology or if they intend to pass some or all of the liability on to their suppliers. None have publicly commented on the risks of mismanaging the marketing of self-driving technology.

New Underwriting Challenges

How will auto policies evolve as technology advances? The shift in liability from the vehicle owner to the manufacturer will likely negate the need for the liability portion of a traditional commercial or personal auto policy. Restructuring of auto policies for limited liability and additional physical damage coverage is one way insurers can stay on top of the trends in the auto industry.

Managing Physical Damage Claims

The potentially high cost of replacement parts for self-driving cars likely will affect the physical damage portion of insurance policies. The current base auto liability coverage form (ISO CA 00 01 03 10) provides $1,000 for replacement of permanently installed electronic systems or electronic systems critical for the operation of the vehicle. In the past, these components were not considered critical to auto functionality, so higher limits were not necessary.

As auto technology progresses to Level 4 autonomy, electronic systems will become critical. The components that allow the vehicle to act independently must function properly. Exclusions 4 and 5 of the physical damage coverage section in the ISO CA 00 01 form can be revised to only exclude nonessential electronic parts or after-market parts that have been installed but are not critical to the functionality of the vehicle's autonomous features.[8]

The Cyber Liability Connection

The addition of a cyber liability component into base forms or by endorsement could become an option for insurers. This component would cover corporate or individual risk related to ransomware or information privacy. As the technology advances, individuals and corporations will rely on computer systems and electronic information. Vehicles could be used as tools to track and study information, such as road conditions, route development, or improvement or personal driving habits, creating opportunities for third parties to access this data to steal or hold it for ransom. Personal and commercial automobile-specific cyber liability policies would assist with the recovery and protection of this information.

Potential Impact to Policy Ratings and Insurance Rates

In addition to prompting changes in policy forms, partially and fully automated vehicles pose new challenges to policy rating. Insurance companies have started to offer drivers telematics devices to monitor habits like miles driven, location, speed, near misses/hazards, weather, and crashes. The collected data can ultimately affect auto insurance rates.

The insurance industry hopes that collecting this data will provide a larger data set for safety analysis and revisions of rating models. Experts estimate that a large auto insurance company can rely on a data set of 100 to 150 billion miles driven to produce credible results.[6] It takes time to build a data set of this size. Telematics may be a tool that would provide a wealth of data as vehicle production moves from Levels 1 through 3 that would help insurers and governing agencies monitor statistics on different types of autonomous features. These systems could also help in the gathering of data to help underwriters determine what coverages are necessary to develop or revise when moving from a Level 3 vehicle to a Level 4 vehicle.

However, states have data privacy laws that prohibit insurers from using some types of data to rate policies or for research purposes, making the use of the information collected difficult to access for complete studies. Insurers may shift from rating based upon driving records to rating on location, vehicle replacement cost, and most traveled routes. These factors more directly affect the cost to repair or replace a vehicle.

DRIVING TOWARD THE FUTURE

Autonomous vehicles will slowly become a mainstream form of transport. As this shift happens, we can expect to experience benefits such as reduction in oil consumption, reduced emissions, and fewer auto-related fatalities. At the same time, additional challenges will arise. The hazards associated with owning and operating vehicles are likely to transition from driver error to product defect, as the technology requires less human control. Awareness of security vulnerabilities and liability shifts will help guide the insurance industry in the development of new solutions that help mitigate the risks related to owning, operating, or producing autonomous vehicles.

REFERENCES

1. NHTSA: http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development. Accessed: 9/2/2016.
2. *WIRED*: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Accessed: 9/2/2016.
3. Business Auto Coverage form. CA 00 01 03 06. ISO Properties, Inc., 2005.
4. "Your next car will be hacked. Will autonomous vehicles be worth it?" The Guardian. 13 March 2016. https://www.theguardian.com/technology/2016/mar/13/autonomous-cars-self-driving-hack-mikko-hypponen-sxsw Accessed: 8/26/2016.
5. *Autonomous Vehicles: Considerations for personal and commercial lines insurers.* Munich Reinsurance America, Inc. 2015.
6. "Self-Driving Cars and Insurance." Insurance Information Institute. July 2016. http://www.iii.org/issue-update/self-driving-cars-and-insurance. Accessed: 1/13/2017.
7. *Harvard Business Review*. "The Right and Wrong ways to Regulate Self-Driving Cars." 6 December 2016. https://hbr.org/2016/12/the-right-and-wrong-ways-to-regulate-self-driving-cars. Accessed: December 7, 2016.
8. Kogut, Christine K. "Manufacturers of autonomous vehicles should be making a SPLASh to manage risk." Milliman. August 2016.
9. *New York Times* "Tesla's Self-Driving System Cleared in Deadly Crash." January 19, 2017. https://www.nytimes.com/2017/01/19/business/tesla-model-s-autopilot-fatal-crash.html?smid=nytcore-ipad-share&smprod=nytcore-ipad. Accessed: 23 January 2017.

© 2017 Lockton, Inc. All rights reserved.
KC: 27874

LOCKTON