Analysis of Autonomous Vehicle Safety Constraints Based on Systems-Theoretic Process Analysis

Zongmei Hu*
Guangdong Mechanical & Electrical Polytechnic, Guangzhou, China
*Corresponding author: 398932370@qq.com

Abstract. This article starts with the safety challenges faced by autonomous vehicles, sorts out the development stages of autonomous vehicles and the cases of safety threats. It combines the safety standards of connected vehicles through case analysis, and uses STPA to analyze unsafe controls. Based on the four dimensions of laws, regulations, hardware, software, and network, this paper analyzes the safety constraints of autonomous driving technology, and proposes corresponding safety constraint strategies. The analysis results show that the improvement of the automobile life cycle safety regulation system, the establishment of a new type of anti-deep learning algorithms, and the construction of big data control links by OEMs can effectively reduce the safety risks of autonomous vehicles, which is worth further experimental research.

1. Introduction
Autonomous Vehicle (or Self-driving Automobile) is a smart and self-driving car that can realize it through a computer system [1]. It relies on the cooperation of artificial intelligence, visual computing, radar, monitoring devices and Global Positioning System (GPS) to allow computers to automatically and safely operate motor vehicles without any human initiative. Autonomous vehicles have the following advantages: reducing the fatality rate of vehicle traffic accidents, alleviating traffic congestion and reducing air pollution by adjusting their own driving speed, relieving the problem of difficult parking through reserving and reducing the space on the side of the car to save garage space, reducing driver parking and pickup time, reducing the driver's daily driving time and so on.

2. Basic classification and technical principle of self-driving automobile

2.1. Basic classification of autonomous driving phase
According to SAE (International Association of Automotive Engineers), automation level classification and description are shown in Table 1.

Self-driving cars have become a focus area for the automotive industry and the whole society. As known in Table 2, autonomous driving technology will enter the L4 level in 2020.
| SAE Level | Name                | Description                                                                                                                                                                                                 | Steering, Acceleration and deceleration | Driving environment monitoring | Complex dynamic driving | Supported road conditions and driving modes |
|----------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|---------------------------------|------------------------|-----------------------------------------------|
| 0        | non-automation      | All driving tasks are controlled by human drivers. Under the specific driving mode, the assisted system controls steering or acceleration or deceleration according to environmental information, and expects human drivers to complete all other dynamic driving tasks. | Human driver                           | Human driver                    | Human driver           | No                                            |
| 1        | assisted driving    |                                                                                                                                             | Human driver and system                 | Human driver                    | Human driver           | Partial road conditions and driving modes    |
| 2        | partial automation  |                                                                                                                                             | System                                  | Human driver                    | Human driver           | Partial road conditions and driving modes    |
| 3        | conditional autonomous driving | Autonomous driving systems complete all dynamic driving tasks in specific driving modes, but expect human drivers to properly respond to requests and take over control. | System                                  | System                          | System                | Partial road conditions and driving modes    |
| 4        | highly automation   | Autonomous driving system complete all dynamic driving tasks in specific driving modes. Autonomous driving system can complete all dynamic driving tasks.                                                     | System                                  | System                          | System                | Partial road conditions and driving modes    |
| 5        | full automation     | Autonomous driving system can complete all dynamic driving tasks under full time, all road conditions, and environmental conditions.                                                                   | System                                  | System                          | System                | All road conditions and driving modes        |
2.2. Basic technical principle of self-driving car
Self-driving technology includes video cameras, radar sensors, and laser rangefinders to understand the surrounding traffic conditions, and to navigate the road ahead through a similar map (a map collected by a driver's car). It is generally believed that the technology is divided into three major levels: the perception layer, the cognitive and decision-making layers, and the control layer. Basic technical principle is shown in Figure 1.

![Figure 1. Basic technical principle diagram of self-driving car](image)

3. The status of self-driving cars
American industrial designer Norman Bel Geddes first performed the concept of "Self-driving"[3]. Since then, domestic and foreign automobile giants, research institutions, universities, and internet giants (such as Apple, Google, Baidu, etc.) have participated in the development of autonomous driving technologies [4].

At present, the R&D of self-driving technology is mainly divided into two camps: one is Tesla, Audi and other car companies, and the other is Google, Baidu and other Internet companies. Taking Google and Baidu camp representatives as examples, the development status and future efforts of the two typical representative companies in self-driving technology are described, as shown in Table 2.

From the analysis of the current technology development status of major car companies and research institutions, it is known that the typical architecture characteristics of self-driving cars are:

1. IT attributes become more obvious. Each car has up to 100 ECUs, runs more and more lines of code (over 200 million lines for self-driving cars), and is equipped with more and more sensors. All-electronic and network have become a trend.

2. Highly interconnected with the outside world. Connect other vehicles and connected devices, third parties and user devices, and use cloud services to process big data.
Table 2. Comparison of Baidu and Google development of self-driving cars

| Internet business representative | Development goal | Development situation | Technology development trend |
|----------------------------------|------------------|----------------------|-----------------------------|
| Baidu                            | Small-scale commercialization within 3 years; Mass production will be achieved within 5 years (2021). | In 2013, self-driving vehicle project was launched. In July 2014, first release of "Baidu self-driving vehicle", developed self-driving vehicle retains steering wheel and pedals. In Sept, announced cooperation with BMW. In 2015, the self-driving division was established, and for the first time in Dec., fully automated driving under mixed conditions of urban, ring road and highway. In Mar.2016, officially released the "Smart Car Strategy" and signed a strategic cooperation agreement with Chang’an Automobile. In Sept, at the Baidu World Congress, the L3 division was officially announced to study applications in both high-speed and parking scenarios. At the 3rd World Internet Conference, Baidu self-driving vehicles debuted in Nov. In Jan. 2017, at the International Consumer Electronics Show (CES), an exhibition stand was set up with Chang’an Automobile to showcase Chang’an Ruifeng self-driving car. | Continue to optimize the self-developed vehicle computing center and existing CPU + GPU + FPGA computing platform; Continue to upgrade and build its core named Baidu automotive brain. |
| Google                           | Don’t advocate building car; Take "robot system" as the development goal of full autonomous vehicles. | In 2009, self-driving vehicle project was launched. In 2011, the Lexus RX450H SUV was converted into a second-generation self-driving car. In 2012, the company obtained the road test license for self-driving cars in Nevada, and affixed the card to a modified Toyota Prius. In May 2014, the third-generation self-developed self-driving car was released. In Oct. 2016, test vehicles equipped with the new autonomous driving system were tested in many locations in the United States with extreme weather. In Dec. 2016, the self-driving company Waymo was established; and it announced that it would jointly develop fully autonomous driving technology with Honda. In 2018, Waymo tested 600 vehicles on the road and the tested total mileage exceeded 16.09 million kilometers. The tested mileage provided a lot of data for deep learning networks. | Continue to accumulate technologies in deep learning, data collection and modeling. |
4. Self-driving car challenges

Because of two typical characteristics, hacking and information interaction will cause serious hidden dangers in information security challenges. Table 3 includes property security, privacy security, life security, and social security. Four dimensions of cases were collected.

| Safety class     | Typical case                                                                 | Danger grade                                                                 | Technical blind spot                                                                 | Live picture |
|------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------|
| property security| In 2015, Charlie Miller & Chris Valasek remotely cracked Chrysler's "JEEP Free Light" | Forced to recall 1.4 million cars due to hacker risk, and caused economic losses | hacking attack                                                                    |              |
| privacy security | In 2015, researchers from two European universities said that through wireless modules and antennas, all vehicles in a small city could be tracked at a cost of less than $500,000. | Owner information leaked  
In 2013, well-known American journalist Michael Hastings died in a car accident. Prior to his death, he received suspected threatening emails, and conspiracy theorists speculated that his vehicle was controlled by a third party. | Information interaction process leads to security risks |              |
| life security     |                                                                 |                                                                                       |                                                                                     |              |
| social security   | In 2016, the US FBI official website reported that the well-known terrorist organization ISIS is researching self-driving car bombs and applying them to suicide bombers. |                                                                                     | Hacking               |              |

Table 4 lists from a series of security risk events to the generation of the world's first automotive cybersecurity standard SAE J3061. The recommended procedure "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" is the first for automotive cybersecurity. The guidance document is designed to promote the establishment of safety processes between automotive electrical systems and other interconnected systems by unifying global standards.
Table 4. Security risk event

| Time    | Event                                                                 |
|---------|----------------------------------------------------------------------|
| 2010.03 | United States Texas GPS Tracking Event.                               |
| 2011.03 | Comprehensive experimental analysis report of the car attack surface at the University of Washington. |
| 2011.09 | DEF CON hacker conference, SMS unlocked Subaru Outback.              |
| 2013.09 | DEF CON hacker conference, OBD-II controlled the steering wheel, brakes, and throttle of Ford Mavericks and Toyota Prius. |
| 2014.04 | 360 company said that Tesla's car operating procedures are flawed.   |
| 2014.08 | A research report at the Black Hat conference pointed out that many well-known automotive electronic systems have security risks. |
| 2015.02 | Universal Anjixing cracked, hackers can "locate, unlock and remotely start". |
| 2015.02 | Ed Markey's Office Releases "Vehicle Connectivity Security Vulnerability Research Report". |
| 2015.07 | Fiat Chrysler recalls about 1.4 million cars.                        |
| 2015.08 | 360 vulnerability platform exposes BYD cloud service crack.          |
| 2016.01 | The world's first automotive cybersecurity standard- SAE J3061.       |

The SAE J3061 defines a structured network security process framework in detail to guide the construction of computer systems with extremely high security requirements. The entire standard has always emphasized the system engineering of automotive network security, that is, information security should be considered in the system design from the beginning of the project, and effective protection should be provided throughout its life cycle, that is, throughout the product design, R & D, manufacturing, maintenance, recycling, and other links.

Self-driving cars are the product of technological changes in automobiles. The technological changes in automobiles have developed along the intelligent, electrified, and connectivity. Table 5 lists the technical safety hazards in the process of automotive technology change. If these safety hazards are not properly solved, they will restrict the development of autonomous vehicles.

Table 5. Automotive technology changes and security risks

| Automotive technology change | Security risks                                                                 |
|------------------------------|--------------------------------------------------------------------------------|
| Intelligent                  | A self-driving car runs more than 200 million lines of code, the program is more complicated. Adopting perception-decision-control instead of human direct control over mechanical parts, social security problems may be caused by hidden information security risks. |
| Electrification              | The PLC circuit of the charging pile control module is connected to the management system via Ethernet, which lacks protection within the entire network. Attacking BMS control algorithms to affect battery performance of electric vehicles. |
| Connectivity                 | Inherited security flaws of existing computing and networking architectures. The vehicle information system is interconnected with the outside world, the index of shared information increases, and information leakage involves user privacy and security. |
5. Self-driving car technology under the framework of STPA

5.1. Basic framework of STPA
Nancy Leveson [6] proposed the systems-theoretic process analysis (STPA) method in 2011. Safety was regarded as a control problem, and the goal was to identify those inadequate controls that might cause dangers. Reduce the risk to an acceptable level [7]. The specific process framework of STPA is shown in Figure 2.

![Figure 2. STPA process](image)

STPA analysis starts from specific accidents, analyzes dangerous events, and derives system-level safety constraints, that is, requirements for system behavior safety in order to avoid or mitigate the harm caused by dangers. Then, the unsafe control behavior is identified from the control structure, and the cause analysis is performed to provide a safety constraint basis for the vehicle control safety constraint.

5.2. Analysis of "unsafe control behavior" of self-driving car

(1) Analysis of dangerous behaviors in the control process of autonomous vehicles
The analysis of the dangerous behavior of the self-driving car control process is shown in Figure 3. Because self-driving cars have high-value attack targets, so control parameters and privacy data have a high attack value. Driving machine decisions replace manual decisions, which increases the danger. Information devices such as sensors and intelligent control are used extensively, and the system is complex. Reliability of communication protocols may have certain loopholes, then the risk of information increased. V2X wireless communication will bring new information security issues, unauthorized access to internal and external interfaces, wired and wireless interfaces or have the possibility of invasion. These unsafe controls can lead to danger.

![Figure 3. Analysis of "unsafe control behavior" of self-driving car](image)
(2) Hazard analysis of the use of self-driving car
The self-driving car itself, driving environment, automatic monitoring, and fault repairing are all facing dangerous behaviors, as shown in Figure 4.

The existing simple defense cannot prevent deliberate invasion, and the current dangerous behavior is actually the behavior of information security protection and management. The challenges we currently face have also inspired our research directions, as shown in Table 6.

Table 6. Dangerous challenges and enlightenment of self-driving car

| Challenges                                                                 | Enlightenment                                                                 |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Standard OBD interface allows access to automotive networks and even updates ECU firmware. | How to defend when anyone has access?                                         |
| Attacker could use legitimate credentials to attack car.                  | How to handle a potential attack?                                             |
| Threat detection of vehicle information is necessary, but there are false positives. | How to determine if the vehicle threat information is false positive?        |
| ECU security credentials must be exchanged securely with each vehicle.    | How to securely manage the exchange credentials of all ECUs when large-scale intrusion is to be prevented? |
| Serious consequences happened once a car is invaded.                     | How to deal with critical attacks?                                            |
| Car equipment has many functions and connects to different networks.      | How to ensure the safety of the software and applications of the on-board system? |
| The solution must be considered in multiple dimensions, such as secure connection, management of security credentials, etc. | How to support the safety management of thousands of cars?                   |

5.3. Analysis of control constraints for self-driving vehicles
The safety problem of autonomous vehicles, that is, the control problem in STPA, this method also considers the dangers caused by non-failures such as software and hardware failures and performance limitations. It is mainly reflected in the safety of self-driving vehicles during driving, mainly including: hardware safety (mainly refers to the safety of on-board sensors, on-board chips, actuators and other components), software security (refers to the on-board decision-making system that can ensure the
correct steering, acceleration, reduction and parking based on the collected driving data) and network security (refers to whether the design of the relevant car networking system can protect self-driving cars from cyber attacks, or the driving functions due to cyber attacks are not affected). Hardware security is the foundation, software security plays a decisive role, and network security is the biggest risk. Therefore, they complement and influence each other. R & D personnel must explore and research more in these three safety aspects to improve the safety of self-driving cars.

(1) Establish automotive information security standard system based on automotive life cycle, emphasizing process constraints

The relevant state ministries and commissions should formulate the development path of intelligent vehicle information security and promote the establishment of corresponding specifications, standards and systems. At present, the standard system is under construction, and various auto manufacturers mainly recommend standards. Some official standards such as "Technical Requirements for Vehicle Gateway Based on Public Telecommunication Network", "Intelligent and Connected Vehicles On-board Terminal Cyber Security", "Information Classified Security Protection Requirement for System of IoTPS" (GB/T 35317-2017), "Security Technology Requirements for Sensing Terminal Access to IoTPS" (GB/T 35592-2017), "Security Protection Technology Requirements for Sensing Terminals of IoTPS" (GB/T 35318-2017), etc [8]. The implementation of these standards must be combined with the safety requirements of the automobile life cycle, as shown in Figure 5.

![Figure 5. Automotive life cycle standard](image)

(2) Establish automotive software and hardware safety constraint control based on the analysis of automatic driving control parameters

(a) Hardware security constraints: the sensor’s perception ability control. The system's unsafe control behavior is mainly caused by signal loss, delay or misjudgment caused by hardware failure, such as Tesla's first fatal accident, mainly because its sensor camera was misjudged by the environmental impact. It is developed, which has the characteristics of greater detection distance and low cost, and which is not affected by smoke or direct sunlight. It has a high-resolution, zero-false-positive, and highly reliable sensing system to ensure that it is not affected by random environmental changes to fail.

(b) Software security constraints: improve the software functions of the decision-making system. The unsafe control behavior of the system is mainly caused by control instructions that are output incorrectly due to algorithm calculation errors. Neural network algorithms are used to effectively control control parameters. Collect the input information through the camera, throttle position sensor, etc., and establish a linear relationship between the input information and the output.
Where, \( x \) is input value, \( W \) is weight vector, \( b \) is offset value.

By solving equation (1), a highly coupled relationship is obtained. Even if the information is difficult to express with a simple mathematical model, the law is found from the observation data samples, and the learned law model is used for unknown or unobservable data. For prediction, the neural network model is shown in equation (2):

\[
f(x) = G(b^{(2)} + W^{(2)}(s(b^{(1)} + W^{(1)} x)))
\]  

(2)

When the training data is insufficient, it is easy to overfit, and it is impossible to capture all the rules of the data when facing a large amount of data. Deep learning uses more layers of parameters to greatly improve the ability to fit a large amount of data [9]. Using millions of parameters to analyze the inherent laws of the data, it is not easy to appear overfitting. It can automatically detect abnormal conditions. Even if this model has not appeared before, it does not require artificial design features. Features can be automatically selected and the input information is hierarchically expressed. The deep learning model is shown in equation (3):

\[
h_{ij}^{k} = \tanh((W^{k} \cdot x)_{ij} + b_{k})
\]  

(3)

The construction of a new type of adversarial deep learning algorithm can quickly analyze the size of the data, the quality of the data, and the characteristics of the data itself, reduce the calculation time, and improve the accuracy of the algorithm.

(c) Network security constraints: multi-dimensional means strengthen network security precautions. If a virus invades, it can cause the internal control system to get out of control, the software decision-making system will be directly affected, the car will be manipulated at will, and even the hardware safety will be affected. Therefore, the storage and transmission of existing big data and the collection and use of information must be effectively protected, and security precautions such as big data encryption, gateway anti-virus, and intrusion detection must be strengthened to effectively prevent the system from being attacked by vulnerabilities to cause various accidents.

Connected big data security is the biggest risk of network security. The level of connected big data technology will also be the key to the development of self-driving car technology in the future. The links that automotive companies need to control are shown in Figure 6.

![Figure 6. OEMs control.](image)
6. Conclusion

(1) Human driving is replaced by automatic machines, which increases the risk of attack on data such as control parameters and privacy data, and is the source of unsafe control factors for autonomous vehicles.

(2) Establishing automobile life cycle safety standards and forming a closed-loop regulatory system will help improve the system safety process control of self-driving vehicles.

(3) Improving the reliability and control progress of sensors is the basis for implementing system process control.

(4) Build a new type of adversarial deep learning algorithm, which can reduce the calculation time, improve the accuracy of the algorithm, and improve the accuracy of security control.

(5) The enterprise constructs control links to realize real-time management of big data, which can effectively prevent data attacks.

Acknowledgments

This work was financially supported by 2019 Guangdong Provincial Department of Science and Technology-Platform Environment Project(2019A141405030).

This work was financially supported by Key Research Platforms and Research Projects of Colleges and Universities in Guangdong Province in 2018 fund(2018GkQNCX122).

Zongmei Hu (1983-), Female, Postgraduate, Master’s degree, a lecturer in Guangdong Mechanical & Electrical Polytechnic. Research direction: automobile electronic control technology, braking performance evaluation.

References

[1] Fan Quanyong, Jin Maojing, Huang Ling, Wang Xuechao, Cao Yaoguang. Safety problems and countermeasures of self-driving cars[J]. China Science and Technology Business, 2019, 6 (6) 13-15.

[2] Sun Baoming. Analysis of self-driving vehicle technology[J]. New Technology & New Products of China, 2019, 9 :15-16.

[3] Wang Fang, Chen Chao, Huang Jianxi. Research Review of self-driving vehicle[J]. China Water Transport, 2016, 16(12), 126-128.

[4] Yang Yanming, Gao Zenggui, Zhang Zilong, Shen Yue, Wang Linjun. Research on Development Strategy of Unmanned Driving Technology[J]. Engineering Sciences, 2018, 20(6): 101-104.

[5] Lan Jing. Development situation and key technology of self-driving cars[J]. Internal Combustion Engine & Parts, 2019, (15): 209-210.

[6] Leveson N. Engineering a Safer World: Systems Thinking Applied to Safety[M]. MIT Press, 2011.

[7] Chen Junyi, Zhou Tangrui, Xing Xingyu, Xiong Lu. Research on Safety Analysis Method for Autonomous Vehicles Based on STPA[J]. Automobile Technology, 2019, (12): 1-5.

[8] Luo Yingluo. Automotive Cyber Security Standardization Status Update[R]. China Academy Information of and Communication Technology, 2016.

[9] Wang Jian. Analysis and Countermeasures of Vehicle Network Information Security[R]. Tsinghua University, 2016.