UWill Discover Conference

UWill Discover 2022

# Safety in Automated Vehicles

Nandini Patel
*University of Windsor*, patel23l@uwindsor.ca

# Safety in Automated Vehicles

A new perspective in understanding how people can trust the choices a system makes

Nandini Patel
University of Windsor
patel23l@uwindsor.ca

***Abstract* — Day by day, automated vehicles are becoming complex whether that is their connection to different networks, to the internet of things, or simply in security and safety for users. The more intricate automation becomes, the more safety needs to mature. There is safety in the software of systems however the bigger concern lies in ensuring the safety of the drivers and passengers. Whether a person is a contributor to the automation industry or a user of automated products and services, it is important to ask some critical questions. Does the industry have enough knowledge or has there been enough research and experimentation done to allow such a complex system to make decisions whether that is as simple as heating the car for a few minutes before going in or something big as changing lanes on a highway where cars are speeding? The purpose of this paper is to explore the different ways in which people can trust such systems and for those who can begin to start trusting.**

***Keywords* — ISO 26262, Electric Vehicles (EV), Automotive Security, Functional Safety, DevSecOps, Automated Driving System (ADS), Advanced Driver-Assistance Systems, Automated Vehicle (AV), Static Application Security Testing (SAST), Automotive Safety Integrity Level (ASIL), Society of Autonomous Engineers (SAE)**

## 1. Introduction

In modern life, everything runs on code – it would not be wrong to say that life runs on code. Though code makes tasks simpler and autonomous, the idea itself creates a high risk in the safety and security of the processes and people. Once the consumers are satisfied with that, they can take a step forward in understanding the core and convincing reasons behind relying on AVs. Security and safety are two concepts that are commonly misunderstood hence, need to be distinguished.

## 2. Automotive Security

Security in automation refers to the branch of the computer that focuses on the cyber risks that are involved in the cases. In today’s day and age, cyberattacks are likely to occur between systems or attacks to emerge from components of a large system. So much of the world’s attention is now diverted to next-generation connected vehicles from scooters to sports cars that the issue of cyber safety has become prominent.

Autocrypt is one of the two companies in the world providing end-to-end security in AV. The director of Autocrypt, Sean Cho, said that “we have found more than 10,000 hacking scenarios in electric and autonomous vehicles and I’m sure there are more” [9]. The fact that every vehicle contains thousands of data leak points is not surprising. Each of these links poses a security threat that needs to be dealt with – each leak with its priority level. Automotive security is exactly that – an approach to building a secure environment for a system where developers can efficiently deal with data leak points in a manner.

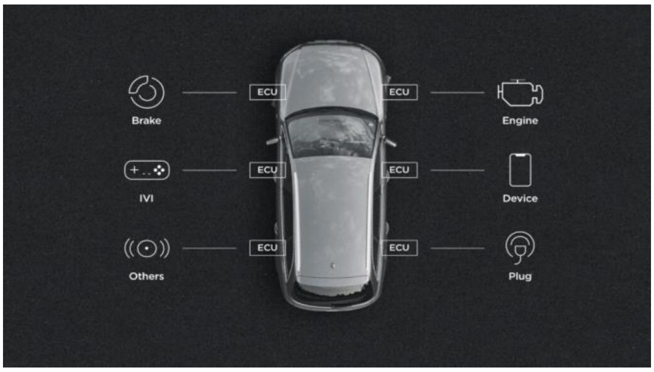

Fig. 1: From smartphone devices to EV chargers, cybersecurity vulnerabilities exist within so many connected vehicles [9]

## 1. Functional Safety

Functional safety is the absence of risk due to hazards caused by failures or unintended behaviors of electrical and electronic systems. Prevention involves strictly following many standards and management within the systems. There are international standards called ISO 26262 containing guidelines to protect drivers, pedestrians, and other road users from injuries that are caused by faults in vehicles whether that is in electronics or software. The ISO 26262 has 11 sections providing detailed insight about customer safety: Vocabulary, Management, Concept Phase, System Level, Production/Operation, Hardware, Software, Motorcycles, Supporting Processes, Safety Analyses, Guidelines, and Semiconductors. In most cars, there is a cruise control feature that could lead to electronic fault. Software fault includes uncontrolled acceleration, which can lead to a tragedy. Functional safety aims to reduce risks on the road and set guidelines that society finds acceptable [2].

According to the ISO 26262, management of functional safety is essential – this is achieved by working structurally. This includes ensuring that companies have clearly defined and applied strict development procedures. Along with this, a trained safety manager is required who oversees planning and managing safety activities. The procedure also involves creating a safety case stating why the system is safe. Other tasks similar to this are part of the standards ensuring that driving risks are minimized as much as they can [11].

After understanding the two core ideas, one can attempt to see how they relate. Safety can become a concern if security does not exist during the process. In other words, if risks are not identified soon enough, unintended behaviors can result whether that is machine-related – not intended by humans– or system-related – intended by people i.e., hijacking.

In vehicles, specifically cars, these two factors are crucial because more and more cars are adapting the autonomous approach. Due to this, the industry is facing many challenges that create room for doubt for their customers. This could be because of several reasons i.e., lack of awareness in public, limited research, learning from experiences of their close ones.

Toyota, Volvo, Tesla, General Motors (GM), and many others are all automotive companies. According to Statista, Tesla was ranked as the best-selling electric vehicle manufacturer worldwide. Volkswagen Group and GM were among the runners-up [4].

Tesla has been proven to be the most reliable in public demand hence, one can focus more on Tesla as a company to understand its challenges, car structure, policies, and other relevant factors.

## 2. The Misuse Challenge

### 2.1 Factors [1]

- Vehicle Owner – Users can activate features that are unpaid or unreleased, manipulate or fake record data impacting mainly safety and privacy
- Installers/Third Parties – Can motivate to repair, activate features in the system, change parameters of functions, bill new components impacting safety, privacy, and customer trust
- Hacker – Rejection of function requests, denial of service manipulation of the shutdown, stealing personal data impacting safety
- Terrorist – Through remote control, use vehicles as weapons, cause intentional accidents, bring down critical infrastructure impacting mainly safety and infrastructure damage.

Noticeably, security hence safety is heavily affected by all these factors. Then how do individuals rely on these systems? There were almost close to 421,000 units of Tesla sold just in the first half of 2021 [4]. The sales must mean that reasons to rely on such interconnected systems overweighs its risk. To understand those reasons, one needs to first examine the processes of how AVs are built.

### 2.2 DevSecOps Automation

Though DevOps is a common concept, one should understand it briefly. DevOps aims to make the software delivery cycle efficient with rapid changes in business requirements. Fast delivery allows organizations to better serve their customers as well as compete better in the market. DevOps is integrated into three key areas: process, people, and products. Continuous Delivery (CD) and Continuous Integration (CI) is an important part of DevOps that helps to deliver the code fast and securely. It is a method that builds, tests, and deploys code using automation [5].

Usually, DevOps is a process on its own and so is security. Both have their cycles but with the rapid pace of code changes, it is hard to keep up with both cycles. When both cycles are separate, security becomes an after-check rather than an integrated check within DevOps, which would be ideal as that practice would save lots of time and would prevent high risk.

Millions of lines of code are written every day for these autonomous vehicles. Upon completion of a feature or product, there are automated tests, builds, deployment and the cycle continues. But what about security within the cycle? In some applications related to vehicles, it is important to ensure there are no security holes in the system. DevSecOps Automation is key for safety-critical software development where the aim is to be secure in the default state and this process is adopted into the automotive industry. A key practice of DevSecOps is creating security as a code practice and integrating it into the day-to-day development tools.

In a nutshell, DevSecOps in automation is integrated security tools in code culture into the DevOps pipeline. When diving deep into the specifics, every PR passes through security scanning and policies, there is continuous integration built from the main branch, a test is done where security and vulnerability tests must pass 100%, and only then, the code is deployed across the stages.

A key part of this process is using a tool called Static Application Security Testing (SAST) – also known as the white-box testing – to detect vulnerabilities. Familiar or not, SAST is a valuable tool for writing quality code. SAST takes advantage of having the code by looking through the source code of an application for any security defects or any other different issues to identify vulnerabilities. This is applied using SAST vendor tools such as Checkmarx, Veracode, Micro Focus, which can be integrated with the CI/CD pipeline for that application. After every commit, SAST performs a scan giving the developers a quick and upfront of the security posture.

## 3. The Current State Of Art

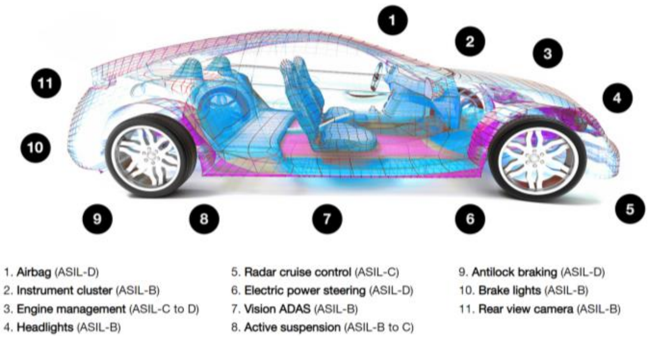
1
2
3
4
5
6
7
8
9
10
11
1. Airbag (ASIL-D)
2. Instrument cluster (ASIL-B)
3. Engine management (ASIL-C to D)
4. Headlights (ASIL-B)
5. Radar cruise control (ASIL-C)
6. Electric power steering (ASIL-D)
7. Vision ADAS (ASIL-B)
8. Active suspension (ASIL-B to C)
9. Antilock braking (ASIL-D)
10. Brake lights (ASIL-B)
11. Rear view camera (ASIL-B)

Fig. 2: ASIL-Related System – a risk classification scheme defined by ISO 26262, which is the safety standard for electronic devices [2]

To understand why these vehicles are safe to drive physically, one should begin by looking at how cars are structured. Electric cars do not have an engine. During an accident, when the steel and aluminum of a car in the front crumbles, it absorbs much of the impact, preventing it from being transmitted to the passengers.

Along with that, these vehicles are difficult to roll over because they have a low center of gravity since the heavy battery pack and electric motors are set low in the vehicles. In the case where it does roll over, cars like Tesla rely on the strength of its roof to protect the occupants. Tesla Model 3's roof has been proven to resist more than 20,000 pounds of force, which is 6 times its weight.

In Oregon recently, in November 2020, the driver of model S crashed into a pole hitting two trees. The impact of this accident was so severe that hundreds of small batteries that work together to power Tesla came apart on the road. Despite the damage, the driver walked away with only a minor injury. When looking at the image, one can see that the driver's seat was almost in place [3].

Another interesting way of thinking about an autonomous vehicle is one of the major components of its build is to engineer it in such a way to prevent accidents, allowing people to rely on it.

To continue, Tesla is researching to assess whether a driver is safe enough to perform autonomous tasks. Specifically, the system is taking advantage of its connected nature to collect useful data. Some of that includes "tracking the number of forwarding collisions warnings per 1,000 miles, hard braking events (above 0.3 G), any aggressive turning (above 0.4 G), whether the driver follows other vehicles too closely (within 1 second), and any forced autopilot disengagements" [12].

All this data is used to better understand the behavior of drivers and to understand how systems should be modified for the future. Research and experimentation have been done to understand how individuals are handling their autonomy.

## 4. Decision Making

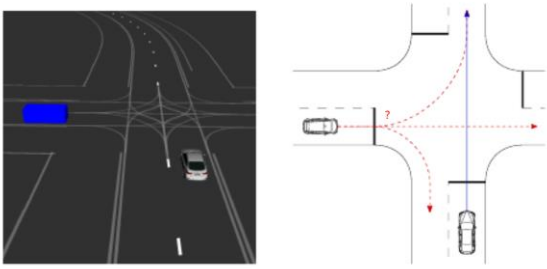

Fig. 3: A situation where the vehicle must decide for action despite the uncertainty of the future [8]

Autonomous vehicle requires independent decision-making in all different types of environments. A car might have to change lanes on a busy highway or decide which way to turn based on what is provided in the GPS.

Advanced Driver-Assistance Systems (ADAS) collect data from inside and outside the vehicle through several sensors. This helps to provide warnings to the driver or help in general during the driving process. Recently, ADAS has shown huge improvement towards autonomous driving.

ADAS has been an approach that is adopted into the vehicle market to prevent accidents. According to a survey, 98% of road accidents are caused by human carelessness. In that 90% can be prevented if a warning is provided, preferably 2 seconds in advance. Here is where ADAS is most used.

There are two ways in which ADAS can be used: passenger acting based on the system's warning and system acting based on its best understanding of the system. For the first method, the system can provide warnings i.e., when the car is too close, the windshield needs to be clear, or anything related to the cameras. And for the second method, in Figure 3, the white car is speeding straight when the driver, which is us, in blue is going straight. If both cars proceed to go in the direction, they are moving, they will collide. To prevent such scenarios, using the ADAS system, the blue car will stop if the navigation advises going straight. In other words, ADAS decides for the occupant.

Despite this, some situations remain ambiguous as not all cases are discovered. More cases that drivers experience, the stronger the decision-making becomes. However, that involves risks for those experiencing it for the first time. Such situations can be a dilemma whether the system should prioritize the driver's safety by maybe hitting a vehicle to minimize the danger of going with the road and getting hit which could mean sacrificing the driver's life. Here is where the regulations play a big role.

## 5. Regulations On Connected & Automated Vehicles

There are levels of autonomy when it comes to driving:

- Level 0 – No Driving Automation
- Level 1 – Driver Assistance
- Level 2 – Partial Driving Automation
- Level 3 – Conditional Driving Automation
- Level 4 – High Driving Automation
- Level 5 – Full Driving Automation

In Ontario, there are automated vehicle pilot programs allowing drivers to operate under levels 4 and 5 under pilot mode. Levels 0 to 3 can be driven by the public however strict regulations are applied on higher levels. Having these standards allows not only the drivers to be safe, but also for the companies to incorporate safety standards. SAE level 3 vehicles can be driven in Ontario under the following conditions [11]:

1. The driver should take back the driving task when prompted by the vehicle
2. Drivers are expected to be always in full control of the vehicle
3. Existing laws of impaired driving and distracted driving laws are in full effect for these drivers
4. Driver must be always in the driver's seat
5. The vehicle must be overseen by a passenger remotely

An important thing to notice here is regardless of which level of driving it is, always during a trip, the driver must be present in the driver's seat. This means that in the end, if any dangerous situation arises, the system is there to assist with the knowledge it has collected from its surroundings and of the system itself, the occupant has the final call to make the decision.

Here, customers need to understand the strength of autonomous systems. They provide people with a decision rather than a reaction that we would be making if we are driving non-autonomously. During a critical situation where the driver has less than 2 seconds to decide, it is safe to say that the call is the instinctual panicked move rather than a deliberation decision. Not to mention, accidents can and still are bound to happen as it's in the nature of driving.

## 6. Conclusion

Some people are excited at the prospect of autonomous tasks while others are terrified. Building security software is crucial to protect the application and its feature so there are no problems in the future. Safety is on the line when security is at risk. Many misuse challenges are faced as a result such as hacking into the system, terrorists taking control over the actions, third-party installations, and more. Autonomous driving must not exist without solid security. There are certainly reasons to be concerned with AVs, all of which are valid. However, the automotive industry has done both research and experimentation to prove that the benefits outweigh the risk.

DevSecOps is a crucial process that is integrated to quickly recognize any data leaks and resolve them before deploying the code. Specifically, SAST is used to scan the source code and detect any vulnerabilities. Furthermore, there has been evidence showing that structurally, electric cars are capable of handling accidents they are designed in such a way. Knowing this, allows customers to trust autonomous vehicles because hundreds or thousands of test accidents have been performed, with different surroundings or cases. To continue, decision-making has been the toughest area of this subject as there is no guideline that a system follows to make decisions. Rather, it is specific to the situation. This is done using a cutting-edge technology called ADAS that collects data from internal and external surroundings to provide warnings and guidance to the driver.

From country to country and within different provinces, there are standards that autonomous vehicle drivers must follow to comply with the law. In Ontario, Canada, and other provinces, all conditions ensure that the driver will be always present in the car and will have the last call in making the decision. Trust plays a large role. A system that has learned several cases from the past likely has more information than the driver about the roads, traffic, and other factors can offer suggestions. It is up to the driver to believe that this can be the right act. Blindly believing the system would be a foolish act. Hence, it is always smart to consider the system’s decision *as well as* put your own experience and understanding of the current situation to make a well-informed decision. Only then, safety can be incorporated to its best in autonomous vehicles.

## Acknowledgment

The accomplishment of this persuasive paper benefits from the help and direction from a professor – Dr. Ikjot Saini as well as other researchers, who have provided insightful views of autonomous vehicles and related ideas.

## References

[1] https://dl.gi.de/bitstream/handle/20.500.12116/2456/13.pdf?sequence=1&isAllowed=y

[2] https://www.micron.com/solutions/automotive/functional-safety-for-automotive#:~:text=Functional%20safety%20is%20the%20absence,of%20electrical%20and%20electronic%20systems

[3] https://insideevs.com/news/455369/stoned-driver-tesla-model-3-crash-oregon/

[4] https://www.statista.com/statistics/541390/global-sales-of-plug-in-electric-vehicle-manufacturers/#:~:text=Tesla%20was%20ranked%20as%20the,share%20of%20about%2015%20percent

[5] https://www.researchgate.net/publication/348288718_DevOps_phases_across_Software_Development_Lifecycle

[6] https://www.researchgate.net/publication/318812740_Decision_making_for_autonomous_driving_considering_interaction_and_uncertain_prediction_of_surrounding_vehicles

[7] https://www.researchgate.net/publication/318812740_Decision_making_for_autonomous_driving_considering_interaction_and_uncertain_prediction_of_surrounding_vehicles#pf8

[8] https://www.ontario.ca/page/automated-vehicle-pilot-program#_Driverless_testing_conditions

[9] https://electricautonomy.ca/2021/08/19/autocrypt-vehicle-cybersecurity/

[10] https://www.blakes.com/getmedia/1cee0d7e-f3ec-429e-ba54-9341506005f4/Blakes_Autonomous_Vehicle_Regulation_in_Canada_0605_EN.pdf.aspx

[11] https://fscdn.rohm.com/en/products/databook/white_paper/iso26262_wp-e.pdf

[12] https://arstechnica.com/cars/2021/09/tesla-tests-drivers-to-trust-them-to-supervise-experimental-autopilot/