Journal of Trends in Computer Science and Smart Technology (ISSN: 2582-4104)
www.irojournals.com/tcsst/

Automated Driving Safety Framework through Security Architecture - Survey

K. Geetha

Dean, Academics and Research, JCT College of Engineering and Technology, Coimbatore

E-mail: geetha.arulmani@gmail.com

Abstract

An enormous wave of automation technology is about to hit the global market. To save thousands of people's lives, autonomous vehicle technology may decrease congestion and increase mobility, as well as may enhance the productivity of the transportation industry. Developed country governments, on the other hand, are concerned that they may be placing unneeded or unforeseen obstacles on the path of growth. As a result, when it comes to features, safety always comes first. With the help of various functions based on certain automation technologies, this effort attempts to find example ideas. A more technical look at the needs throughout the development to minimize safety-related dangers is presented in this paper, which is meant to augment previous publications on different safety elements. This article emphasizes the significance of safety by design. Additionally, the goal of this article is to overcome the problems of the existing system with authentication and security architecture framework.

Keywords: Automated vehicle, cybersecurity, neural network, prediction analysis, autonomous

1. Introduction

When creating Cyber-Physical Systems (CPS) such as linked and autonomous automobiles, security, safety, and privacy aspects merge. Increased connection and automation, as well as changes in the ownership of vehicles, may be a contributing factor. As a consequence, security and safety (as well as privacy) are becoming more intertwined. Fully autonomous cars have a cybersecurity risk since their safety-critical activities rely on external data sources such as, onboard sensors, V2X connectivity, and remote services from cloud servers. As a result, any one of these channels may be breached, causing services to fail or data assets to be lost [1-5]. An integrated engineering approach is required here.

DOI: https://doi.org/10.36548/jtcsst.2022.2.001
Received: 17.05.2022, received in revised form: 02.06.2022, accepted: 16.06.2022, published: 27.06.2022

By cooperating on perceptual and driving-related duties, individual autonomous cars may benefit from inter-vehicle and roadside communication. It is also possible for transportation and law enforcement authorities to profit from real-time traffic information given by every car. There are many transportation system stakeholders that want to reduce the risk of cyber-attacks. V2X misbehaviour detection systems may depend on data from onboard sensors, but they can also take use of information from infrastructure components. From a vehicle- and infrastructure-based viewpoints, cyber dangers are presented and mitigation options are discussed in this study.

Autonomous vehicles need more expensive maintenance due to the risk of catastrophic failure if its components aren't properly fitted and maintained. Advanced driver aid systems (cameras, radar, and ultrasound) cost almost twice as much as minor accident damage nowadays as compared to previous generations [6-8].

1.1 Cybersecurity importance

Automated driving poses new issues for the automobile industry because of the high level of communication inside and between automated driving cars and their operational environment. These difficulties include anything from meeting regulatory standards and safeguarding public safety to prevent cyberattacks on fleets and consumers. Car control functions and many information technology backend approaches with various base foundation will all be linked through new interfaces. Sadly, this wide range of assault options attracts a lot of attention from criminals with a variety of motives. In other words, we've progressed to the point where cars can no longer function safely without also maintaining a safe condition. Mostly, a vehicle's movement can't be taken over by attackers, and scaling assaults to exploit numerous vehicles simultaneously is difficult [9-11].

1.2 Purpose of this article

A major goal of this work is to help standardize autonomous driving throughout the whole industry. A framework or recommendations for mechanical driving system safety is developed as part of this initiative, and it will benefit all enterprises through various industries from suppliers of vital technology.

2. Self-driving car Infrastructure

Automated cars are not self-driving. Public and private (e.g., back-office activities) infrastructure is used to support vehicles. Data collected from an infrastructure are taken into account by autonomous driving cars, but the cars retain control over their own decision-making in the final analysis, not the infrastructure. Automated driving cars must also take into account the people who will be required to operate, manage, repair, etc., these vehicles. Vehicle entry is restricted and compartmentalized depending on the vehicle's intended use. Operations workers, for example, may need to know the location and condition of a vehicle, but they don't need to know who is inside [12,13].

2.1 Safety Measures

Many limited seats cars are explicitly geared on functional safety in these types of vehicles. To determine and convey standard risk, the Automotive Safety Integrity Levels (ASILs) are utilized. ASIL values in conventional applications of functional safety are not traced and decomposed in this paper, but they can be studied from the previous structural behaviour. When it comes to ASIL D's biggest safety hazards, it is well recognized by those involved in operational security that an electrical vehicle defect that causes failures at the system level might lead to erroneous steering or braking.

2.2 Automotive Industry Cybersecurity

Even if they can't explain the connection between the two, people often lump safety and security together. This category is logical because of the overlap between the problems' attributes. While both are concerned with the appropriate operation of a system, their emphasis differs somewhat in the safety focuses of the system's capacity to withstand a purposely malevolent activity. The dangers posed by passive enemies like hostile human beings acting purposefully are the safety and security concerns of the dangers posed towards active opponents. Security is forced to rely on extra tools and methods, which compromise the integrity of the system [14- 16].

2.3 Deep security architecture

In order to meet the previously described security objectives, this section explains how security functions are stacked. There are several layers of protection in place for autonomous cars, starting with the lowest level components (e.g., sensors) and working up to the vehicle itself and the infrastructure that supports it. Data, systems, functions, or components of embedded systems for automatic driving may all benefit from the classic trinity of information security: Confidentiality, Integrity, Authenticity, and Availability (CIA). Confidentiality and integrity may be secured at the component level (e.g., microcontroller/ECU/camera sensors) using primitives. Component tamper resistance, configurability (e.g., the removal or disablement of unnecessary elements) and updatability are also addressed in this article.

3. Proposed Solution

3.1 Fuzzy procedure with sensor fusion

Algorithms and strategies for sensor fusion have been investigated intensively in the past several years. But a modern research found that getting the most recent fusion methods and algorithms is a difficult and time-consuming effort because of the many different fusion algorithms published in the literature. Deep learning device combination methods and conventional sensor fusion algorithms combine neural network classification research. In order to combine sensor data, traditional algorithms including knowledge-based, statistical, and probabilistic sensor fusion rely on notions of uncertainty arising from data flaws, such as imperfection and latency. Proposals for roundabout detection and navigation systems on roads are also being considered. In order to locate objects, it makes use of the suggested "Laser Simulator" technique and the knowledge-based Fuzzy Logic (FL) algorithm [17, 18].

3.2 Deep Neural Network

Input pre-processing procedures like as scaling and resampling may also be included in the DNN-based architecture. The DNN architecture's user interface can only be customized if these stages are included in the design. The DNN is the emphasis of this architectural level. It is important to consider the use case and specification needs when deciding on the kind and mix of DNN layers to include i.e., while deciding the architecture. On the DNN architectural side, issues to consider include the data types and dimensions of the input and output, as well as the model's size and categorization. In addition, the activation function must be carefully chosen, since it is critical to the approximation of the function. The DNN model's convergence may be accelerated as a result of this. In addition, there are a number of DNN architectural features to consider, such as the pooling layer type, stride, recurrence, and more. Furthermore, the network's generalization may be further adjusted throughout the development and evaluation process.

3.3 Training and detection procedure

Labelled data may be used to train a DNN model by applying a loss function that determines how far model outputs depart from the labels. The DNN model's training loss is minimized via back propagation of the associated gradient after averaging the error across (randomly chosen) training dataset samples. Depending on the loss function and regularization used, the resultant network's resilience may vary greatly. Because of this, it may be necessary to limit the number of alternative loss functions that may be used in the training phase. In addition, the cost function is connected to the distribution of the data's numerical values [19 – 22].

3.4 Prediction of objects

Neuronal network output may not be sufficient as input for the safe and legal development of an ambitious goal. A more comprehensive depiction of a dynamic driving scenario, or "scene", is needed to incorporate not just present conditions but also projections for the future. The purpose of other dynamic objects and items that occlusions from view may obscure should also be considered when making predictions about future movements. It is also necessary to consider the present weather conditions, which include impaired sensor performance. Figure 1 shows the block diagram of future behaviour prediction process.

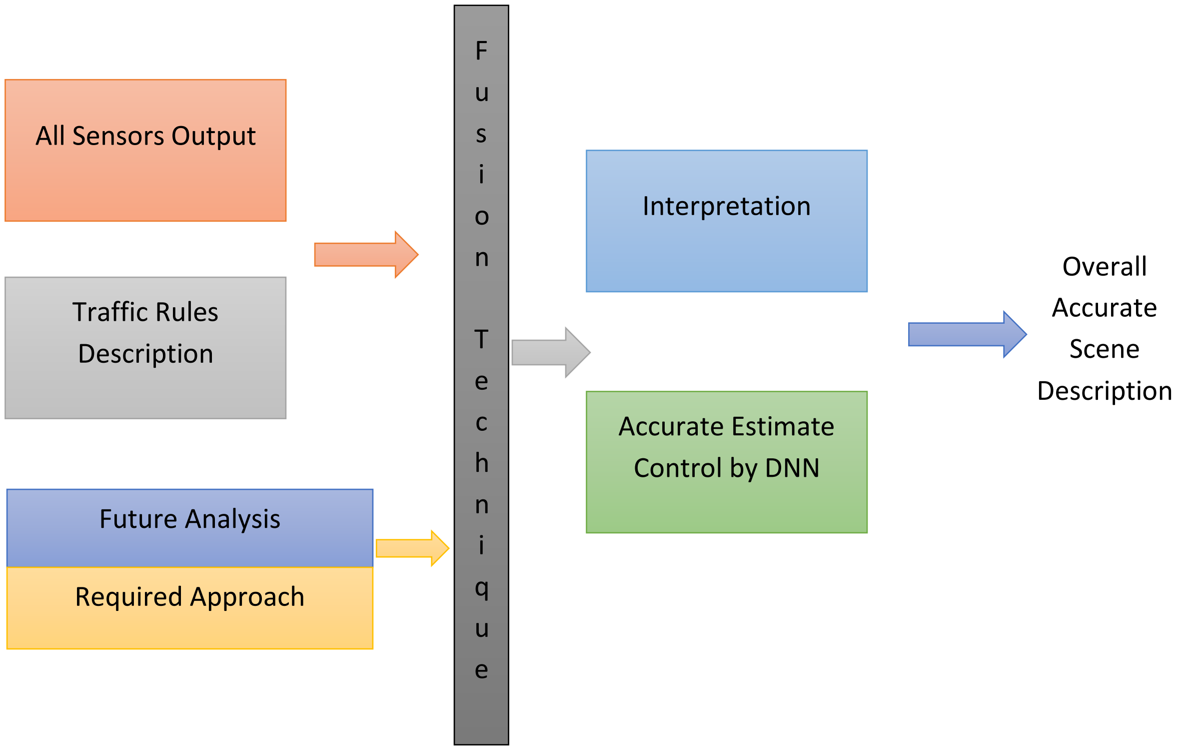

Figure 1. Future Behaviour prediction

3.5 Collision Free driving plan

Many factors must be taken into account while creating a safe and legal driving strategy. Prior to any driving plan, for example, the car must have correctly detected its surroundings and completed localisation. The vehicle should next take into account the world model's safety-relevant (vulnerable) road users recommendations from an construal and estimate calculation viewpoint, once localization has been served and an accurate world model has been supplied. Thus, it is possible to begin making inferences about potentially vulnerable road users [23, 24].

3.6 Localization process

If the automated driving system's intended usage is limited, it must be assured that it performs only within the established system restrictions. This means that utilizing sensor fusion techniques, the automated driving vehicle should be accurately found here. At times, additional prior details from outside of the automated driving vehicles on board perception performance may be required in order to achieve appropriate localization. These details can be from the automated driving vehicle's own range or from an outside source.

Commercial vehicle’s drivers, on the other hand, offer services like passenger assistance and security, as well as loading, monitoring, and maintenance, thus certain positions for vehicle operators will be eliminated. Rapid development, deployment, and fleet turnover are all necessary for a more rapid application of this vehicle technology than has been the case in the past.

3.7 Future predictions

Driverless car implementation is slowed by causes such as the following when it comes to the advancement of technology. In the near future, automobiles will be able to run autonomously under all regular circumstances thanks to Level 4 technology (vehicles capable of self-driving in restricted circumstances). Whether dependable Level 5 operation can be achieved in the next five years is uncertain.

3.7.1 Regulations and testing

While testing and approval standards are now being developed, it may take many more years before they are widely employed. Large-scale testing will take considerably longer.

3.7.2 Increasing expenses

Additional equipment and services are needed for autonomous cars, which increases the overall cost. Only very expensive new cars will be able to drive independently which means that yearly expenditures will rise by thousands of dollars when compared to humanoperated vehicles. This technology will be available in fewer new automobiles due to high extra costs, which will slow down fleet adoption.

3.7.3 Autonomous vehicle sale

The look at how people travel and live as well as their preferences for new developments are provided. Most households in the United States reside in automobile-dependent areas and possess their own automobiles. Autonomous vehicle sharing is best suited for families that travel fewer than 6,000 miles per year by car in more multimodal areas. People who are able to live in multi-modal communities will be more likely to use shared independent vehicles. People may be reluctant to adopt self-driving automobiles because of concerns about safety, privacy, or their own preferences. When the market is fully saturated, consumers will still be able to purchase vehicles. Table 1 contains the autonomous vehicle planning problems [25].

Table 1. Autonomous vehicle planning problems

Performance Measures	Future analysis	Required Approach	Response Duration
Safety and Reliability	Consider safety and dependability. Set up a foundation for regulation.	To decrease congestion, accidents, and pollution, transportation management is needed.	Moderate
Travel Comfort	Consider the possible advantages and expenses of changing trip plans.	Decongestion pricing, vehicle limits, priority, and regulations that encourage sharing a trip.	High
Traffic from local roads	Investigate the effects of shifting patterns in the volume of automobile traffic.	Disability- and low-income-inclusive policy for the use of AVs.	High
Safety	New dangers and collision repercussions, especially for other road users, should be	Regulate and promote the use of self-driving cars and trips in public spaces.	High

	examined.		
Non-Driving mobility	Rides and transportation services provided by self-driving cars	Encourage the use of Alternative Vehicles (AVs) that are both efficient and electric. Manage roads to reduce the number of vehicles on the road.	High
Impacts on use of shared vehicle	Type and use of AV gasoline.	Curb space and parking needs may be minimized by reducing parking regulations.	High
Environmental and monetary costs	Overall vehicle travel is affected by this.	Redesign the road layout. Create AV lanes if required.	Moderate
Passenger loading at parking	Vehicles, as well as parking and loading requirements.	Find out how much money they have and how much they'll charge.	Moderate
Design for highway	To what extent other road users have to contend with the presence of AVs	Minimize conflict and danger using rules and facility designs.	Moderate
Preparation of traffic type	Effects on traffic flow and the design of the route.	All road users' safety depends on regulating autonomous vehicles. and safe road management.	High
Needs of self-driving car	Mandating AVs might have certain advantages.	Make all cars autonomous and limit human driving if the advantages are significant enough.	High

3.7.4 Autonomous vehicle demand

Future transportation demands and planning requirements will be influenced by several developments, including the development of autonomous vehicles. Changes in the population, customer preferences, costs, information technology, transit alternatives and other planning advances may be more important than self-driving automobiles in the near future.

4. Descriptions of Datasets

It is expected that the dataset will improve over time as more cases are uncovered, hence decreasing the amount of unknown information. To keep the DNN-trained model as accurate as possible as the dataset's diversity changes over time, it's important that the dataset itself reflects any changes in the operating environment. To keep track of everything from the weather to the sensors' settings, tagging is essential and allows the data is to be rearranged in any way. In certain circumstances, the collection of data may be improved by using various strategies, such as augmentation or synthesis. However, it is essential that the most correct data be the most prominent.

5. Conclusion

Building the autonomous driving product's safety case requires the use of evidence from the aforementioned parts. There should be some thought put into what additional standard working required on a deep neural network; this is important. As a starting point, one may conceive about the proposed neural network's whole development process as detailed previously in the article. The behaviour of an autonomous driving system cannot be precisely described because of the dynamic, ever-changing nature of the surroundings. As a result, the need for real-time monitoring grows. Monitoring DNNs while they are functioning is an important aspect of a successful deployment. Developing accurate and effective obstacle detection in self-driving cars is essential. In order to obtain greatest efficient self-driving cars, this is a must-have feature. Recent research have taken a more pragmatic approach when it comes to obstacle detection, by combining data from several sensors such as distance sensors, velocities and colours that are essential for ensuring the safety and reliability of the system.

References

[1] Ma, X.; Niu, Y.; Gu, L.; Wang, Y.; Zhao, Y.; Bailey, J.; Lu, F. Understanding Adversarial Attacks on Deep Learning Based Medical Image Analysis Systems. arXiv 2020, arXiv:1907.10456v2.

[2] Yurtsever, E.; Lambert, J.; Carballo, A.; Takeda, K. A Survey of Autonomous Driving: Common Practices and Emerging Technologies. IEEE Access 2020, 8, 58443–58469.

[3] Rawat, P. Environment Perception for Autonomous Driving: A 1/10 Scale Implementation of Low-Level Sensor Fusion Using Occupancy Grid Mapping. Master's Thesis, KTH Royal Institute of Technology, Stockholm, Sweden, March 2019.

[4] Kiran, B.R.; Sobh, I.; Talpaert, V.; Mannion, P.; Al Sallab, A.A.; Yogamani, S.; Pérez, P. Deep Reinforcement Learning for Autonomous Driving: A Survey. arXiv 2021, arXiv:2002.00444v2.

[5] Zhou, Y.; Sun, P.; Zhang, Y.; Anguelov, D.; Gao, J.; Ouyang, T.; Guo, J.; Ngiam, J.; Vasudevan, V. End-to-End Mult-View Fusion for 3D Object Detection in LiDAR Point Clouds. arXiv 2019, arXiv:1910.06528v2.

[6] Brena, R.F.; Aguileta, A.A.; Trejo, L.A.; Molino-Minero-Re, E.; Mayora, O. Choosing the Best Sensor Fusion Method: A Machine Learning Approach. Sensors 2020, 20, 2350.

[7] Rosique, F.; Navarro, P.J.; Fernández, C.; Padilla, A. A Systematic Review of Perception System and Simulators for Autonomous Vehicles Research. Sensors 2019, 19, 648.

[8] Y. Zhu, J. Wang, S. Liang, and J. Wang, "Covariance control joint integrated probabilistic data association filter for multi-target tracking," IET Radar, Sonar Navig., vol. 13, no. 4, pp. 584–592, 2018, DOI: 10.1049/ietrsn.2018.5142.

[9] J. G. Wang, S. J. Chen, L. B. Zhou, K. W. Wan, and W. Y. Yau, "Vehicle Detection and Width Estimation in Rain by Fusing Radar and Vision," 2018 15th Int. Conf. Control. Autom. Robot. Vision, ICARCV, Singapore, SINGAPORE, 2018, pp. 1063–1068.

[10] H. Jha, V. Lodhi, and D. Chakravarty, "Object Detection and Identification Using Vision and Radar Data Fusion System for Ground-Based Navigation," 2019 6th Int. Conf. Signal Process. Integr. INDIA, Networks, Noida, 2019, pp. 590–593.

[11] M. Dimitrievski, P. Veelaert, and W. Philips, "Behavioral pedestrian tracking using a camera and lidar sensors on a moving vehicle," Sensors (Switzerland), vol. 19, no. 2, 2019, DOI: 10.3390/s19020391.

[12] F. Harrer, F. Pfeiffer, A. Löffler, T. Gisder, and E. Biebl, "Synthetic Aperture Radar Algorithm for a Global Amplitude Map." 2017 14th Workshop on Positioning, Navigation and Communications (WPNC) 2018 (2017), pp. 1-6, Bremen, Germany, 2018, DOI: 10.1109/WPNC.2017.8250080.

[13] R. Weston, S. Cen, P. Newman, and I. Posner, "Probably Unknown: Deep Inverse Sensor Modelling In Radar," International Conference on Robotics and Automation (ICRA), Montreal, Canada, 2018, pp.5446-5453. arxiv id: 1810.08151.

[14] Kim, Beomjun, et al. "Automated Complex Urban Driving based on Enhanced Environment Representation with GPS/map, Radar, Lidar and Vision." Ifac Papersonline 49.11, pp. 190-195. 2016, DOI: 10.1016/j.ifacol.2016.08.029.

[15] V. Lekic and Z. Babic, “Automotive radar and camera fusion using Generative Adversarial Networks,” Comput. Vis. Image Underst., vol. 184, no. April, pp. 1–8, 2019, DOI: 10.1016/j.cviu.2019.04.002.

[16] B. Yektakhah and K. Sarabandi, “All-Directions Through-the-Wall Imaging Using a Small Number of Moving Omnidirectional Bi-Static FMCW Transceivers,” IEEE Trans. Geosci. Remote Sens., vol. 57, no. 5, pp. 2618–2627, 2019, DOI: 10.1109/TGRS.2018.2875695.

[17] Chia-Ming Tsai ; Yi-Horng Lai ; Jau-Woei Perng ; I-Fong Tsui ; Yu-Jen Chung, "Design and Application of an Autonomous Surface Vehicle with an AI-based Sensing Capability," 2019 IEEE Underwater Technology (UT), Kaohsiung, Taiwan, Taiwan, 13 June 2019, DOI: 10.1109/UT.2019.8734350.

[18] Kim, Jung-Jae, Si-Ho Cha, Minwoo Ryu, and Minho Jo. "Pre-training Framework for Improving Learning Speed of Reinforcement Learning Based Autonomous Vehicles." 2019 International Conference on Electronics, Information, and Communication (ICEIC) (2019): 1-2. Korea, DOI: 10.23919/ELINFOCOM.2019.8706441.

[19] Mehra, A.; Mandal, M.; Narang, P.; Chamola, V. ReViewNet: A Fast and Resource Optimized Network for Enabling Safe Autonomous Driving in Hazy Weather Conditions. IEEE Trans. Intell. Transp. Syst. 2020, 1–11.

[20] Gonzalez-de-Santos, P.; Fernández, R.; Sepúlveda, D.; Navas, E.; Emmi, L.; Armada, M. Field Robots for Intelligent Farms Inhering Features from Industry. Agronomy 2020, 10, 1638.

[21] Velasco-Hernandez, G.; Yeong, D.J.; Barry, J.;Walsh, J. Autonomous Driving Architectures, Perception and Data Fusion: A Review. In Proceedings of the 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP 2020), Cluj-Napoca, Romania, 3–5 September 2020.

[22] A. Asvadi, L. Garrote, C. Premebida, P. Peixoto, and U. J. Nunes, “Multimodal vehicle detection: fusing 3D-LIDAR and color camera data,” Pattern Recognit. Lett., vol. 115, pp. 20–29, 2018, DOI: 10.1016/j.patrec.2017.09.038.

[23] V. Ilic, M. Marijan, A. Mehmed, and M. Antlanger, “Development of Sensor Fusion Based ADAS Modules in Virtual Environments,” Zooming Innov. Consum. Technol. Novi sad of Conf. ZINC, Serbia, 2018, pp. 88–91.

[24] Y. Kang, H. Yin, and C. Berger, "Test Your Self-Driving Algorithm : An Overview of Publicly Available Driving Datasets and Virtual," IEEE Trans. Intell. Veh., vol. 4, no. 2, pp. 171–185, 2019, DOI: 10.1109/TIV.2018.2886678.

[25] J. Oh, K. Kim, M. Park, and S. Kim, "A Comparative Study on Camera-Radar Calibration Methods," 2018 15th Int. Singapore of Conf. Control. Autom. Robot. Vis. SINGAPORE, 2018, pp. 1057–1062.

Author's biography

K. Geetha is presently working as a Dean-Academics and Research at JCT College of Engineering and Technology, Coimbatore, India. Her area of research includes image processing, computer vision, artificial intelligence, optimization techniques, power systems, process control and automations.