Development of ISO 26262 and ISO 21448 Concept Design Process Integration

ISO 26262 and ISO/PAS 21448 Design Process Integration

Xuezhu Yang[1, a], Muxi Li[1, b], Yi Liu[1, c*], Chengrui Sun[1, d], Miao Wu[1, e], Shiying Zhou[2, f]

[1]E&E Research Department of Intelligent Connected Vehicle Development Institute, FAW, China
[2]General Research and Development Institute, FAW, China

[a]yangxuezhu@faw.com.cn
[b]limuxi@faw.com.cn
[c]liuyi7@faw.com.cn
[d]sunchengrui@faw.com.cn
[e]wumiao@faw.com.cn
[f]zhoushiying@faw.com.cn

Abstract. The development of technology has led to the improvement of vehicle safety and the introduction of autonomous driving system. The autonomous driving related system requires various parts such as camera sensors. Various parts are being added to the vehicle, which is making the system more complicated. Safety-related issues are becoming more important to prevent accidents that may occur during autonomous-driving due to errors caused by increased complexity of the system. For the safety of autonomous driving systems, the International Organization for Standardization introduced the ISO 26262 standard to prevent accidents caused by errors in electrical/electronic systems applied to vehicles. Recently, ISO 21448 is being introduced to compensate for the areas that ISO 26262 does not deal with in relation to autonomous driving. In order to implement autonomous driving technology, ISO 21448 is needed because it is necessary to prevent the risk of performance constraints while implementing functions. However, ISO 21448 is a standard under enactment, and it is difficult to apply to the actual development process. Also, ISO/PAS 21448 is applied with ISO 26262 in the actual development process, so consideration for the application of both processes is needed. This paper proposes an integrated process for applying ISO/PAS 21448 to the actual development process. The integrated process is a combination of ISO 26262 and ISO/PAS 21448, and the concept part of the process is strengthened. For the integration of ISO 26262 and ISO/PAS 21448, each process was analyzed and newly constructed to enhance applicability and reduce trial and error of concept development process.

Keywords: ISO/PAS 21448, ISO 26262, Concept Design, Process Integration

H. Wu et al. (Eds.): CSIEDE 2022, ACSR 103, pp. 121–133, 2022.
https://doi.org/10.2991/978-94-6463-108-1_15

1 Introduction

The development of technology is accelerating the development of advanced driver assistance systems (ADAS) and autonomous driving technologies to improve vehicle safety. And the issue of safety of vehicles due to new system is also increasing. To solve this problem, national agencies such as the New Car Assessment Program (NCAP) are introducing standards to secure the safety performance of vehicles [1-3]. Figure 1 is a roadmap for the features that should be equipped to improve the safety of vehicles presented by Euro NCAP [4-5]. Roadmaps allow checking the introduction and plan of technology to improve the safety of vehicle and support driver [6]. The Society of Automotive Engineers (SAE) defined the autonomous driving phase as 6 steps according to the vehicle function and the role of the driver and system [7]. To implement the technology of autonomous vehicles, cameras, Radar, LiDAR and actuators are required to control them [8-9].

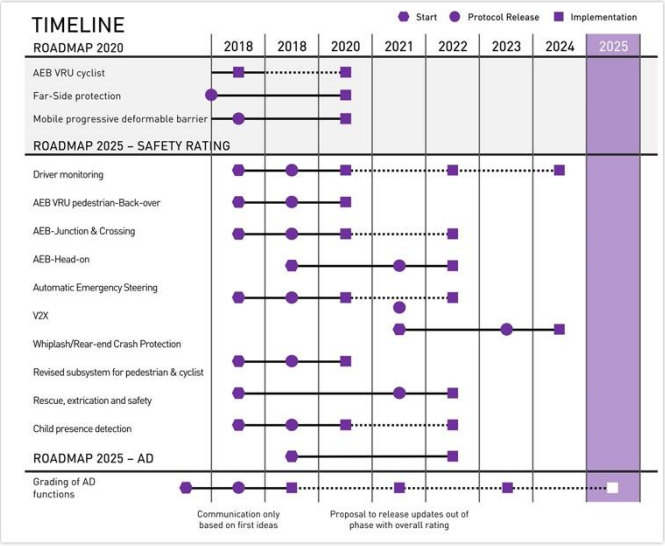

Fig. 1. Euro NCAP's Roadmap for 2018-2025 by Euro NCAP

As a result, the requirements and complexity of E/E systems are increasing, and active research on related technologies is needed to improve the safety of autonomous driving technologies [10-12]. As the level of autonomous driving increases, the driving safety-related judgment of the vehicle is moving from the driver to the vehicle, and many parts and functions are related to accident prevention and safety [13-15]

The Toyota incident showed that there are limitations to quality control in parts suppliers [16]. Tesla's case could confirm that the camera sensor's recognition error could lead to serious accidents [17-18]. The International Organization for Standardization (ISO) introduced the ISO 26262 standard to prevent errors in the electrical/electronic (E/E) system that could occur in vehicles [19]. Recently, ISO 21448 is

being prepared to respond to the development and application of autonomous driving technology [20].

2 Definition of Problem

2.1 Analysis of the limitations of the ISO/PAS 21448

Various advanced functions are being added to the vehicle to implement autonomous driving [21]. ISO/PAS 21448 should be applied to related parts and systems to ensure the safety of vehicles with autonomous driving technology. The Safety of the Intended Functionality (ISO/PAS 21448) was announced by the ISO to prevent unintentionally occurring risks that are not included in ISO 26262 [22].

ISO 26262 proposes an integrated process of the entire development cycle, such as Figure 2, and for the safety of vehicles, ISO/PAS 26262 should be applied with ISO 21448. ISO/PAS 21448 is applied to the entire development process, but in the real industry, the development of functional safety concepts is performed at the concept stage. The development stage performs the technology safety concept and HW and SW development that meet the requirements, but the concept stage is difficult to verify considering the performance limitations and limitations of the product. As shown in Figure 3, ISO 26262 clearly separates the concept stage and the system development stage, but ISO/PAS 21448 has a mixture of the entire process stage.

In the existing process, it is difficult to confirm whether the development process is proceeding in the right direction because the parts suppliers use only the limited information provided from the vehicle manufacturer. This makes it possible to confirm the achievement of ISO/PAS 21448 after the final development, and it is not possible to confirm whether the defined requirements and development process are proceeding accurately. This requires repeating the development cycle until ISO/PAS 21448, and due to time and financial losses, vehicle manufacturers and parts suppliers will be passive in introducing the standard. ISO/PAS 21448 should be applied with ISO 26262, and a process should be formed in which the manufacturer and supplier can carry out the development with the same concept.

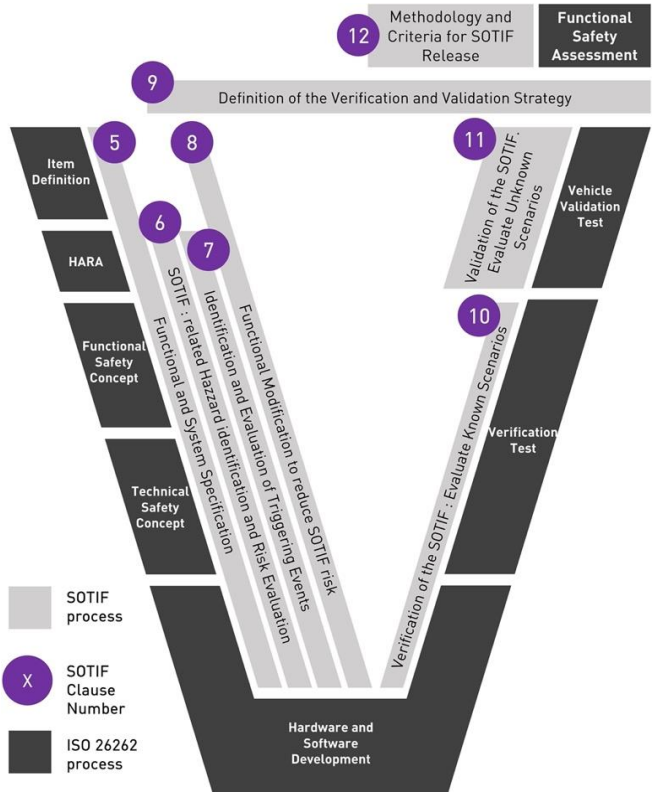

Fig. 2. Relationship between ISO 26262 Process V-Model and ISO/PAS 21448 Process by ISO

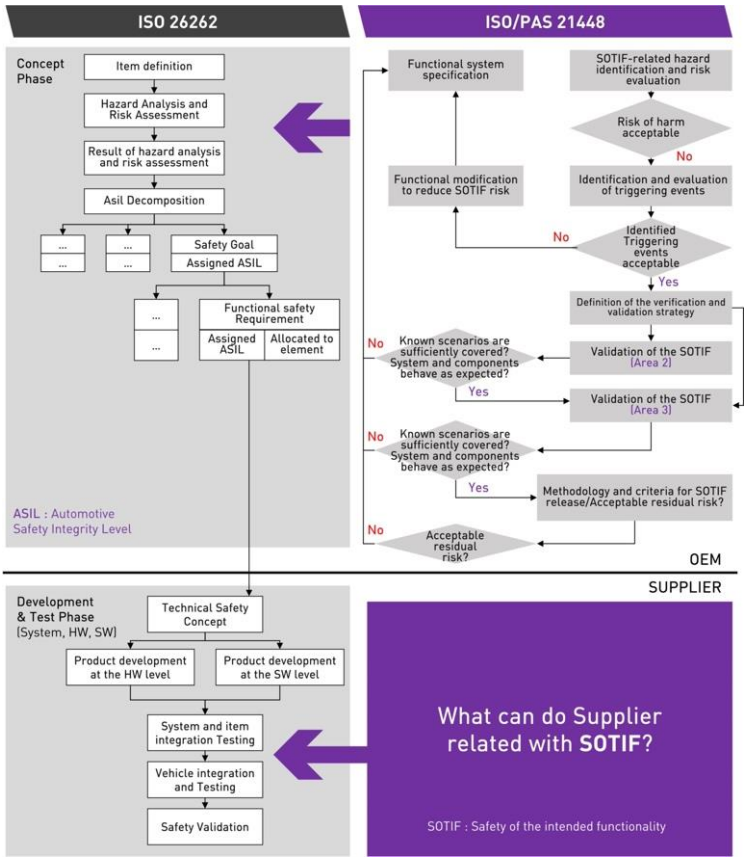

Fig. 3. Supplier's Integration Process Absence in SOTIF and ISO 26262 Design Process by ISO

2.2 Related work for ISO/PAS 21448

Various studies have been conducted related to ISO/PAS 21448. Although the study on ISO/PAS 21448 analysis was conducted, it was limited to the lack of consideration for the development process because it was concentrated on the design of autonomous vehicles [23]. The ISO/PAS 21448 process was organized and the study on the development of the framework was carried out, but it has limitations that it was focused only on scenario derivation and framework [24]. A study of the scenario of ISO/PAS 21448 for the safety of autonomous vehicles was also carried out, but it had limitations that it was focused on the operating environment and scenario [25]. In order to apply ISO/PAS 21448 effectively, it is necessary to analyze and study the entire process of ISO/PAS 21448 along with intensive research and improvement plan for each stage.

For effective application of ISO/PAS 21448, the overall process is needed to be analyzed and studied, and consideration of ISO 26262 is also needed.

3 Integration of ISO 26262 and ISO/PAS 21448

3.1 The Need for Integration of ISO 26262 and ISO/PAS 21448

Research on ISO 26262 and ISO/PAS 21448 was also conducted, but it was limited to the integration of the level of matching the output of individual processes, which did not show much difference from the existing standards [26]. The safety engineering phase of autonomous vehicles was applied to ISO26262 and ISO/PAS 21448, but the process was designed from a safety perspective rather than the system development process and it has limitations in application [27]. Although ML based study was proposed according to ISO 26262 and ISO/PAS 21448, there is a limit to the lack of research and analysis on ISO/PAS 21448 [28]. Precedent studies have shown that there are many studies related to ISO26262 and ISO/PAS 21448, but there are not enough studies to integrate the two processes. As shown in Figure 4, ISO/PAS 21448 is difficult to integrate because the division is not clear compared to ISO 26262, but the integration and application of the two processes must be performed for the safety of the E/E system of the camera sensor used for autonomous driving function.

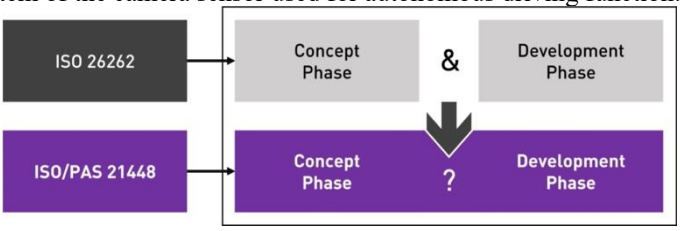

Fig. 4. ISO/PAS 21448 Improvement Requirements

3.2 Objectives and Scope

This study proposes an integrated process to improve problems that arise when ISO/PAS 21448 is applied to autonomous vehicles and components used for function implementation. The study performs the analysis of ISO 26262 and ISO/PAS 21448, such as Figure 5, identifying the relevant matters, identifying the requirements for the existing process, and deriving improvements.

Fig. 5. Objective and Scope

For this purpose, the study analyzed the two processes and identified the related matters to identify the requirements for the existing processes and derive improvements. In addition, the proposed integrated process was intended to clarify the safety requirements in the concept development stage and to clearly distinguish the roles of manufacturers and suppliers.

4 ISO 26262 and ISO/PAS 21448 Integrated Improvements

4.1 Analysis for the Integration Process Derivation

It is important to increase the clarity of the concept phase and system development of ISO 26262 and ISO/PAS 21448 for the response and safety of variables related to autonomous driving and to construct scenarios for risk. ISO/PAS 21448 aims to make the risky scenario Known Safe Area 1 to cope with the danger, as shown in Figure 6.

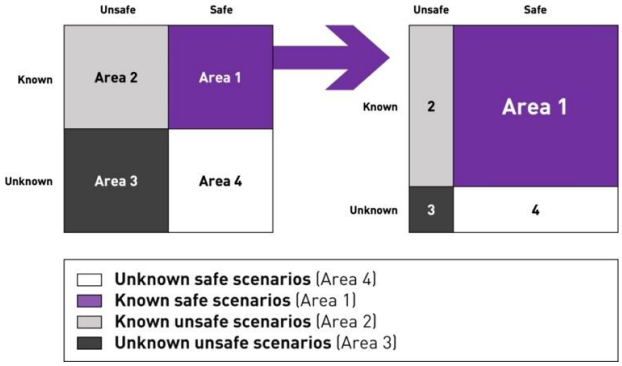

Fig. 6. Safety Goal Concept by ISO

ISO/PAS 21448 deals with scenarios with a wide range of risks and unclear and differs from ISO 26262 because it performs development processes assuming the capabilities of the components or the capabilities to be applied to undefined situations. This results in development using only limited information, and the result of the safety goal achievement confirmation process at the end of the entire development cycle is made. An integrated process is needed to use both standards together to reduce the

development period and cost loss of components applied to autonomous vehicles and ensure safety.

4.2 Integrated Design of ISO 26262 and ISO/PAS 21448

In order to develop parts that meet the safety of ISO/PAS 21448, parts suppliers must participate in the ISO/PAS 21448 process related to the development of actual products, along with vehicle manufacturers. Also, the parts suppliers should develop through accurate role setting, and the vehicle manufacturer should design specific and certain requirements. In this paper, we propose an integrated process that divides the concept stage and development stage of ISO 26262 and ISO/PAS 21448, such as Figure 7. The proposed process specifically proposes an integrated process that can be applied to the concept stage and development stage of the ISO/PAS 21448 process and adds a process to the concept development unlike figure 3, which shows the existing process. The process of the proposed ISO/PAS 21448 can be confirmed in detail through Table 1.

The integrated process focused on the concept development process to carry out the embodiment of the output, use case and safety goals derived through ISO/PAS 21448, clarifying the unclear situation and defining the scenario situation. The purple part (2,3,4,6,7,8) of Figure 7 is the result of further suggestions while integrating the two processes, and it has been defined the detailed factors and risk sources that may arise through this to set safety goals. The improved process can be used as a prerequisite for HARA analysis of the system by defining the related system through assumptions for the top system and assuming parts for related matters such as vehicle movement. In addition, the simplification of the system simplifies and integrates the problems that may arise in the final system to derive results. The proposed process can save time and money by reusing the results of the existing process when the same work is repeated through the circulation structure.

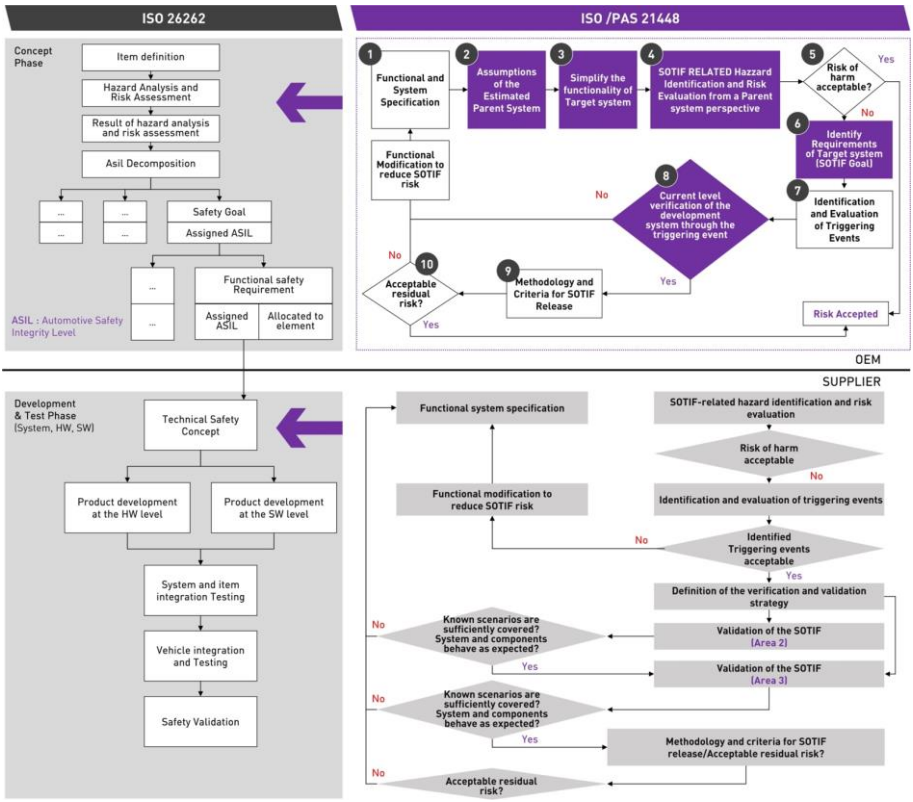

Fig. 7. Proposal for the Improved ISO/PAS 21448 Process with ISO 26262

Table 1. Proposed ISO/PAS 21448 Process Step

No	*Steps*	*Detail*
1	Functional and systematic requirements	To define the development requirements for scenarios, define functional safety requirements and system functional requirements by considering both ISO 26262 and ISO/PAS 21448.
2	The assumption about the top system assumed	Based on Use Case, Scenario, and Scene, the effect of the development system on the upper system(vehicle) is assumed.
3	Simplification of the functionality of the system to be developed	To analyze the risk, divide the representative situation with several characteristics and derive simplified results.
4	Confirming the cause of the risk associated with ISO/PAS 21448, and assessing the risk	The risk associated with the ISO/PAS 21448 target is evaluated through system functions, simplified results and higher system assumptions.
5	Determining whether the risk is acceptable	Whether the risk source of system is acceptable or not decides through the derivation result of the previous step.
6	Deduction of requirements for development systems	The safety goal of system is established through the derivation result of the previous step.
7	Identification and evaluation of Triggering events Triggering	It is used as a bad condition to analyze the factors that can affect the performance of the system and to cause the performance degradation of the system.

8	Verification of Concept Level by Triggering Event Triggering	The second stage scenario and the seventh stage event are applied to the system developed and verification is performed.
9	Methodologies and standards for the distribution of ISO/PAS 21448	
10	Determination of whether the remaining risk is acceptable	

5 Verification of Proposed Process

To verify the improved ISO/PAS 2144 process proposed in this study, we used camera development sensor simulation applied to autonomous driving function. The proposed process was verified based on the camera sensor simulation, such as Figure 8. In terms of parts, we defined requirements for applying the higher system and the ISO/PAS 21448 process to apply the process. In addition, we defined and analyzed factors that can affect the use case creation, function simplification, and safety goals.

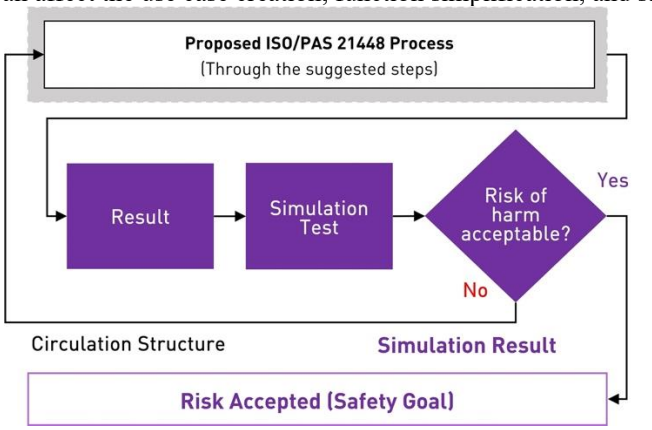

Fig. 8. Verification Process through Camera Sensor

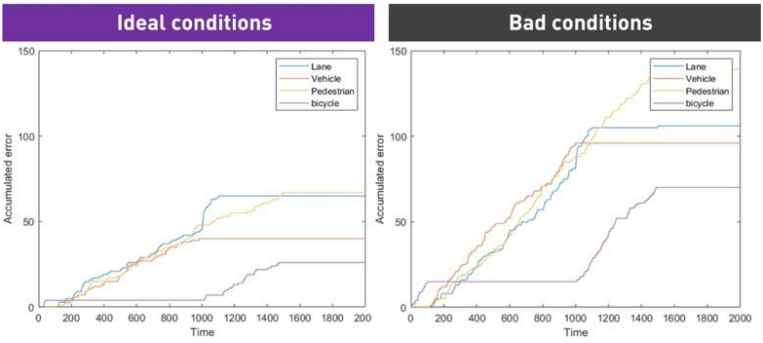

Fig. 9. Camera Simulation Results that Meet Requirements

Simulation results show that using a single camera does not meet the requirements, and if using three cameras, it meets the requirements. Figure 9 is the result of ideal

and bad conditions of camera sensor simulations and confirmed to meet the requirements derived through the proposed process.

6 Conclusion

This study proposed an improved ISO 26262 and ISO/PAS 21448 integration process to secure the safety of components used in autonomous driving related functions. The proposed improved ISO/PAS 21448 process embodied the role definitions and information required for the entire development cycle of the process for the development of parts such as camera sensors. In addition, the proposed ISO/PAS 21448 process was designed to simplify the factors affecting the function and apply it to the development process. In addition, the study tried to contribute to reducing the development cost and period by suggesting a cycle process that can utilize existing results while repeating the process to meet the requirements in the development process. The prosed process is confirmed to be able to derive the results that meet the requirements through camera sensor based simulation.

This paper is to contribute to the increasing safety problem with the arrival of autonomous driving technology. With the development of technology, standards related to robots, aviation, and drones are also being discussed in addition to autonomous vehicles. It would be a good idea to apply ISO 21448 to implement safer and more reliable autonomous mobile technology in each field. In the future, we will carry out follow-up research to increase the objectivity and reliability of the process for the development of related technologies in various fields related to ISO 21448.

References

1. Pereira. N. Q, and Callaghan. B. A, “Comparison New Car Assessment Program NCAP Requirements and Procedures Around the World,” SAE Technical Paper 2013-36-0499, 2013.
2. Hobbs. C. Adrian, and McDonough. Paul. J, “Development of the European New Car Assessment Programme (Euro NCAP),” Transport Research Laboratory, Vol. 44, No. 3, 1998.
3. Paine. M, Paine. D, Case. M, Haley. J, Newland. C, and Worden. S, “Trends with ANCAP safety ratings and real-world crash performance for vehicle models in Australia,” Proceeding of 23rd ESV, 2013.
4. Euro. N.C.A.P, “Euro NCAP 2025 roadmap: In pursuit of vision zero,” Leuven, Belgium, 2017.
5. Walker. J, and Johnson. C, “Peak Car Ownership: The Market Opportunity of Electric Automated Mobility Services,” Rocky Mountain Institute, 2016.
6. Takács. Á, Drexler. D. A, Galambos. P, Rudas. I. J, and Haidegger. T, “The Transition of L2–L3 Autonomy through Euro NCAP Highway Assist Scenarios,” IEEE 17th World Symposium on Applied Machine Intelligence and Informatics (SAMI), 2019, pp. 117-122.
7. “SAE J3016 Levels of driving automation,”. SAE International, 2021.
8. Bebel. J. C, Raskob. B. L, Parker. A. C, and Bebel. D. J, “Managing complexity in an autonomous vehicle,”. Proceedings of IEEE/ION PLANS, 2006, pp. 356-365.

9. R, Heinzler. P, Schindler. J, Seekircher. W, and Ritter. W, Stork, “Weather Influence and Classification with Automotive Lidar Sensors,” 2019 IEEE Intelligent Vehicles Symposium (IV), 2019, pp. 1527-1534.
10. Divyajeet. Bajpayee, and Jitendra. Mathur, “A comparative study about autonomous vehicle,” In: 2015 International Conference on Innovations in Information Embedded and Communication Systems (ICIIECS). 2015. pp. 1-6.
11. Ingle. S, and hute. M, “Tesla autopilot: semi autonomous driving, an uptick for future autonomy,” International Research Journal of Engineering and Technology, Vol. 3, No. 9, 2016, pp. 369-372.
12. Mbowa. K, Aigbavboa. C, Akinshipe. O, and Thwala. D. W, “An overview of key emerging technologies transforming public transportation in the Fourth Industrial Revolution era,” IOP Conference Series: Materials Science and Engineering, Vol. 1107, No. 1, 2021.
13. John. B, Roger. R, Ibrahim. H, Ben. B, John. B, Dave. H, Peter. J, Helen. M, and Robert. P, “Safety cases and their role in ISO 26262 functional safety assessment. International Conference on Computer Safety,” Reliability, and Security Springer, 2013, pp. 154-165.
14. Lim. Gwan-Taik, and Lee. Jae-Chon, “On a Method to Analyze and Verify the Functional Safety of ISO 26262 Based on Systems Engineering Framework,” Journal of the Korea Safety Management and Science, 2013, Vol. 15, No. 3, pp. 61-69.
15. Finkbeiner. M, Krinke. S, Oschmann. D, Saeglitz. T, Schaper. S, Schmidt. W. P, and Schnell. R, “Data collection format for life cycle assessment of the German association of the automotive industry (VDA),” The International Journal of Life Cycle Assessment, Vol. 8, No. 6, 2003, pp. 379-381.
16. Cole. Robert. E, “What really happened to Toyota?,” MIT Sloan Management Review, Vol. 52, No. 4, 2011, pp.29.
17. Banks. V. A, Plant. K. L, and Stanton. N. A, “Driver error or designer error: Using the Perceptual Cycle Model to explore the circumstances surrounding the fatal Tesla crash on 7th May 2016,” Safety science, 2016.
18. Jenssen. G. D, Moen. T, and Johnsen. S. O, “Accidents with Automated Vehicles-Do self-driving cars need a better sense of self?,” In Proceedings of the 26th ITS World Congress, Singapore, 2019.
19. Schnellbach. Adam, and Griessing. Gerhard, “Development of the ISO 21448. European Conference on Software Process Improvement,” Springer, Cham, 2019, pp. 585-593.
20. Okuda. R, Kajiwara. Y, and Terashima. K, “A survey of technical trend of ADAS and autonomous driving,” In Technical Papers of 2014 International Symposium on VLSI Design, 2014, pp. 1-4.
21. Dabral. S, Kamath. S, Appia. V, Mody. M, Zhang. B, and Batur. U, “Trends in camera based automotive driver assistance systems (adas),” In 2014 IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS), 2014, pp. 1110-1115.
22. International Organization for Standardization, “ISO/PAS 21448-Road vehicles-Safety of the intended functionality,” ISO, 2019.
23. Walker. A, “SOTIF the Human Factor. In European Conference on Software Process Improvement,” Springer, Cham, 2019, pp. 575-584.
24. Rau. P, Becker. C, and Brewer. J, “Approach for deriving scenarios for safety of the intended functionality,” In Proc. ESV, 2019, pp. 1-15.
25. Madala. K, Do. H, and Avalos-Gonzalez. C, “A Dependency based Combinatorial Approach for Reducing Effort for Scenario based Safety Analysis of Autonomous Vehicles,” 2021, pp. 235-246.

26. Kirovskii. O, M, and V, A, Gorelov, “Driver assistance systems: analysis, tests and the safety case. ISO 26262 and ISO PAS 21448,” IOP Conference Series: Materials Science and Engineering, 2019, pp. 12-19.
27. Feth. P, Adler. R, Fukuda. T, Ishigooka. T, and Otsuka. S, “Multi-aspect Safety Engineering for Highly Automated Driving,” International Conference on Computer Safety, Reliability and Security, Springer, 2018.
28. Radlak. K, Szczepankiewicz. M, Jones. T, and Serwa. P, “Organization of machine learning based product development as per ISO 26262 and ISO/PAS 21448,” In 2020 IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC) IEEE, 2019, pp. 110-119.