International Journal of Internet, Broadcasting and Communication Vol.15 No.3 219-230 (2023)
http://dx.doi.org/10.7236/IJIBC.2023.15.3.219

IJIBC 23-3-27

Development of ISO 26262 based Requirements Analysis and Verification Method for Efficient Development of Vehicle Software

Kyoung Lak Choi*, Min Joong Kim**, Young Min Kim***†

** Senior Engineer, Automotive Engineering Service Team, DNV GL Business Assurance Korea, Korea*
*** Ph. D. Candidate, Department of Systems Engineering, Ajou University, Korea*
**** Associate professor, Department of Systems Engineering, Ajou University, Korea*
kyoung.lak.choi@dnvgl.com, aquamjkim@ajou.ac.kr, pretty0m@ajou.ac.kr

Abstract

With the development of autonomous driving technology, as the use of software in vehicles increases, the complexity of the system increases and the difficulty of development increases. Developments that meet ISO 26262 must be carried out to reduce the malfunctions that may occur in vehicles where the system is becoming more complex. ISO 26262 for the functional safety of the vehicle industry proposes to consider functional safety from the design stage to all stages of development. Specifically at the software level, the requirements to be complied with during development and the requirements to be complied with during verification are defined. However, it is not clearly expressed about specific design methods or development methods, and it is necessary to supplement development guidelines. The importance of analysis and verification of requirements is increasing due to the development of technology and the increase of system complexity. The vehicle industry must carry out developments that meet functional safety requirements while carrying out various development activities. We propose a process that reflects the perspective of system engineering to meet the smooth application and development requirements of ISO 26262. In addition, the safety analysis/verification FMEA process for the safety of the proposed ISO 26262 function was conducted based on the FCAS (Forward Collision Avoidance Assist System) function applied to autonomous vehicles and the results were confirmed. In addition, the safety analysis/verification FMEA process for the safety of the proposed ISO 26262 function was conducted based on the FCAS (Forward Collision Avoidance Assist System) function applied to the advanced driver assistance system and the results were confirmed.

Keywords: *ISO 26262; Functional Safety; Systems Engineering; FMEA; Autonomous Driving Functions; Software Functional Safety*

1. Introduction

Recently, the electric/electronic(E/E) system has been increasing in various industrial groups due to the development of technology, and in the vehicle industry, the functions that assist drivers through the technology

Manuscript Received: July. 20, 2023 / Revised: July. 24, 2023 / Accepted: July. 27, 2023
Corresponding Author: pretty0m@ajou.ac.kr(Young Min Kim)
Tel: +82-31-219-3949, Fax: +82-31-219-2334
Associate professor, Department of Systems Engineering, Ajou University, Korea

for autonomous driving are being developed and applied. The increase in E/E systems is increasing the complexity of the system and increasing malfunction. Toyota's car accident in 2009 was caused by rapid acceleration due to software defects embedded in the electronic control unit (ECU), resulting in the driver's death [1]. Also, as in Tesla case, it was confirmed that the accident occurred due to the recognition error of the camera sensor [2-3].

The vehicle industry is increasing the development-related requirements due to the development of technology and the application of advanced driver assistance systems (ADAS) functions and technologies for autonomous driving[4]. The design complexity of the vehicle is rapidly increasing due to the increase of the electrical/electronic system, so development to prevent malfunctions should be carried out [5].

Therefore, the vehicle industry related companies established the specialized ISO 26262 functional safety standard in the automobile sector based on IEC 61508 in 2011[6]. Vehicle manufacturers and parts suppliers must comply with ISO 26262 functional safety standards for the development of safety-related electrical/electronic control systems [7]. However, ISO 26262 has limitations in dealing with failures due to interactions between complex systems. It is necessary to study the ways to reduce the malfunction of the vehicle due to the increase in the application of autonomous driving related technology and to meet safety requirements.

2. Definition of Problem

2.1 Functional Safety of ISO 26262

ISO 26262 was officially announced as an international standard with 27 vehicle manufacturers and parts suppliers from 10 countries. The ISO 26262 is applied to systems of vehicles under 3.5 tons and specifies procedures and designs, testing, and safety analysis for each stage of system, software, and hardware development. The composition of ISO 26262 consists of a total of 11 parts, related requirements and recommendations, and the description of each part is the same as Table 1. The functional safety requirement, ISO 26262, is constructed along the systems engineering, such as Figure 1, and it is effective to match the detailed performance to the systems engineering system.

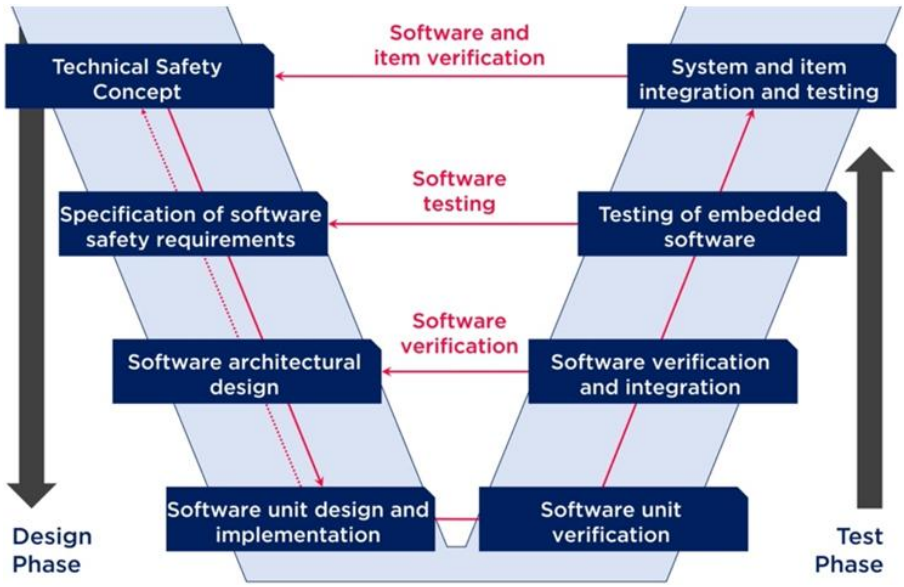

Figure 1. ISO 26262 v-model

Table 1. Configuration of iso 26262 functional safety standard

Part No.	Contents
Part 1. Vocabulary	Terminology theorem used in standard
Part 2. Functional Safety	General safety management after product development and production
Part 3. Concept Phase	Establishing safety goals through hazard analysis and risk evaluation based on item definition
Part 4. System Level Product Development	Development and verification of system levels according to life cycle model
Part 5. Hardware Level Product Development	Development and Verification of Hardware Levels according to Life Cycle Model
Part 6. Software Level Product Development	Development and Verification of Software Levels according to Life Cycle Model
Part 7. Production and Operation	Item production plan, production, operation, disposal
Part 8. Support Process	Safety requirements specification and management, shape management, change management, verification, software tool reliability, software/hardware component recognition
Part 9. ASIL and Safety based Analysis	ASIL for Safety Requirements, Dissolution and Risk Analysis Methods
Part 10. Guideline for ISO 26262	ISO 26262 Major Concepts, Guidelines for ASIL Decomposition, etc.
Part 11. Application of ISO 26262 to semiconductor	Introduction of guide and dependent failure analysis methods and procedures for predicting base failure rate at semiconductor level, concept and method of defect injection test.

In this regard, various studies on ISO 26262 were conducted to secure the safety of vehicles. Focusing on the system engineering V-model connectivity of ISO 26262 research has been conducted on the integration of system engineering and functional safety based on V-model [8-9]. Research has also been conducted to define the phase of system engineering process and safety engineering process and to define the relationship and output of the two processes [10]. However, the previous studies have limitations that they are concentrated on the relationship between system engineering and ISO 26262.

ISO 26262 uses failure mode and effect analysis (FMEA) based on failure mode for functional safety analysis and presents an optimal method for deriving results and ensuring clarity of design verification[11]. FMEA consists of deductive/inductive requirements, such as Figure 2, for system design verification designated in ISO 26262.FMEA, the core item of ISO 26262, should be performed as a product derived from systematic analysis rather than relying on experience for fault data to be dealt with in terms of functional safety [12-13].

	Methods	ASIL			
		A	B	C	D
1	Deductive Analysis [a]	O	+	++	++
2	Inductive Analysis [b]	++	++	++	++

[a] Deductive Analysis Methods Include FTA, Reliability Block Diagrams, Ishikawa Diagram

[b] Inductive Analysis Methods Include FMEA, ETA, Markov Modeling

Figure 2. System design analysis

2.2 Fault Type Derivation Related Work

Studies related to the derivation of fault forms have been preceded. In order to implement effective FMEA, the study proposed the use of individual FMEA forms suitable for the purpose was carried out, but it had a limitation that it could not solve the problem of relying on experience for prediction of failure mode [14]. A study of process flow to accurately identify potential defective modes has also been conducted [15]. In order to identify and the latent defect mode more closely, the method of disassembling the process into work units was explained, but it was focused on the identification of the potential defect mode.

The study of the criteria setting of RPN(Risk Priority Number) severity, incidence and detection was preceded, but only the roundabout problem solving method was presented [16]. Analysis of the failure of the target system is an important factor in the functional safety area of ISO 26262. Requirements related studies were also conducted, and system requirement based TSR(Technical Safety Requirements) derivation studies were also proposed to achieve FSR(Functional Safety Requirements) using use case[17]. Requirements for DIA(Development Interface Agreement) including functional safety factors derived by OEM were also conducted[18], but the specific method of performance was not disclosed without including the performance of suppliers[19]. Based on the actual case of ISO 26262, research on the approach to functional tests, defect injection tests and robustness tests was also conducted. However, the study was focused on the steps associated with testing on the context of ISO 26262 [20].

Studies on the most important aspects of functional safety were also conducted from the ISO 26262 perspective, but they were focused on safety management, development processes, architecture design and safety assurance [21]. Research has also been conducted on methods and technologies to introduce functional safety to autonomous and semi-autonomous vehicles [22]. The study provided an overview of methods and technologies for introducing functional safety to autonomous and semi-autonomous vehicles, but it had limitations that it was concentrated on ASIL(Automotive Safety Integrity Level) of hardware and software. Research has been conducted to provide an overview of methods and technologies for introducing functional safety to autonomous and semi-autonomous vehicles, but it has been focused on analysis of related studies [23].

Various studies have been conducted on the ISO 26262-based fault type derivation, but most of them did not consider the upper system of the analysis level, and the system composition is not considered, so it is difficult to derive clear results.For the application of ISO 26262, analysis should be performed with clear

classification and requirement system between system levels, and fault analysis should be performed through customer requirement analysis and functional analysis of V-model [24].

2.3 Objective and Scope

For the effective application of ISO 26262, the study proposed the system FMEA preparation process, which is a safety analysis/verification method of ISO 26262 Part 4 (Product Development at the system level) based on V-model of systems engineering. The proposed method is not a method of approach at an imitated level, but a methodology that includes demand analysis and functional analysis to be linked to failure. The study presents a methodology to improve the problem that FSR(Functional Safety Requirement) is not systematically organized and data acquisition that depends on past experience and contributes to the development that satisfies ISO 26262.

3. Concept and Definitions of Safety Analysis and Verification Processes

The study proposed a process applied to ISO 26262 using the functional analysis methodology of systems engineering. The proposed process is the same as Figure 2 and consists of a process for safety analysis of the system. The process proposed through the study consists of five steps and the concept and definition of each step are the same as Table 2.

Table 2. Proposed process for systems safety

No.	Conception	Definition
1	Deduction of TSR Initial Concept after Deduction of FSC and FSR	FSC and FSR are the activities of ISO 26262 Part3 Concept phase, the safety goal of the vehicle standard is expressed as FSC, and FSR is derived as the function of the subsystem constituting the system. The activities at this stage should be analyzed considering the interrelationship of the system to be analyzed in the range of the entire vehicle area.
2	Building a component system based on physical definition steps, functional/part analysis charts	TSC should be derived with specific TSR and to draw clear TSR, it is performed to draw results through the linkage of functional block diagram (FBD), FTA, and FMEA.
3	Establishing FTA Level after Detailed Functions Failure Transform	After the functional analysis drawing, the conversion is performed to derive the failure. And the input/output of the functional analysis drawing and the function of the analysis object are arranged in the form of the FTA. The most important system FMEA's purpose item is the cause of failure.
4	FTA Results Based Verification Item FMEA Completion	After three levels of failure (failure impact, failure type, and failure cause) are arranged (written in the form) in FMEA form, design management items are added.
5	Safety Analysis/Verification Complete after Comparison of FMEA Verification Entries and TSR Entries	The results of design verification are drawings and customer requirements, which means that they should be consistent with TSR in terms of functional safety.

The proposed process consists of five steps, with derives the TSR concept after deriving FSC(Functional Safety Concept) and FSR and constructs a functional/part analysis based component system through a physical definition step. Through this we will change the detailed function to fail, establish the FTA level and complete

the verification item FMEA based on the FTA result. It consists of the order of completing safety analysis and verification after comparing FMEA verification items and TSR items. It has been made to contribute to securing the safety of the system through the process. Through the proposed process, customer requirements were derived like Figure 3, and the results were drawn to clearly distinguish by item.

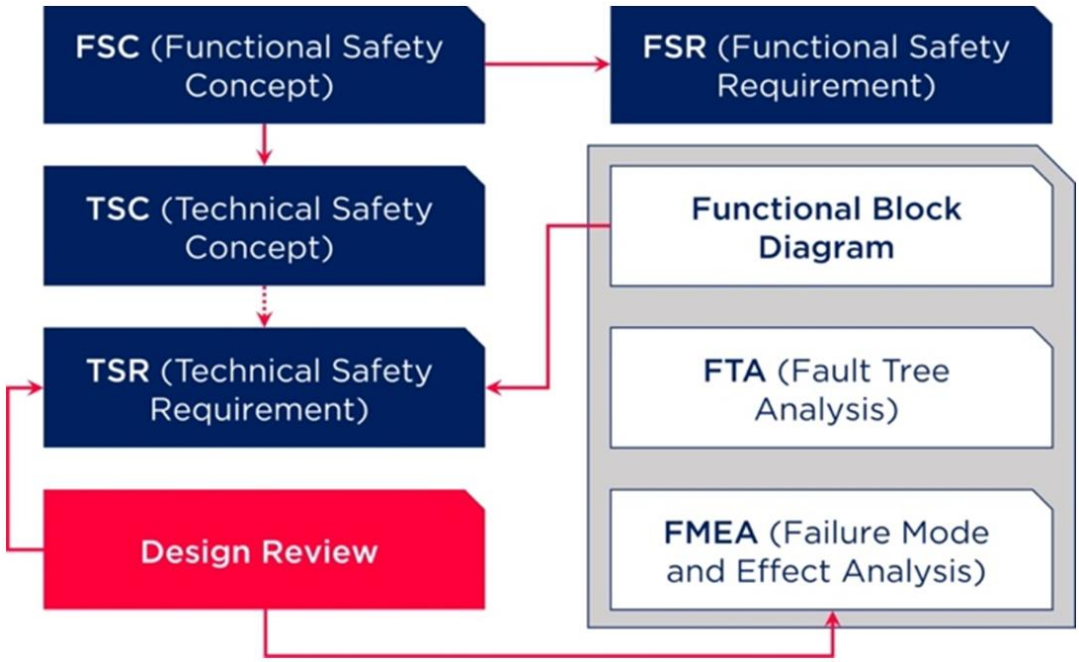

Figure 3. System Safety Analysis Process Concept

4. Safety Analysis and Verification Process Model Validation

The safety analysis process proposed through this study was conducted based on the Forward Collision Avoidance Assist System (FCAS), one of the ADAS(Advanced Driver Assistance System) functions. The safety analysis process was applied to derive and verify TSR to safety FSR, which is presented by the vehicle manufacture as based on 'The braking distance is less than 10km when braking from 50km/h to 0km/h due to the obstacle detection while driving straight on the dry road and it will not collide with the front obstacle.' For this purpose, FCW (Forward Collision Warning) and AEB (Autonomous Emergency Breaking) which are subsystems that constitute FCAS system based on Table 3 were expressed and the component composition for functional analysis was added separately from the linked input/output components.

Table 3. Software requirement description example (ISO 26262-6)

Method		ASIL			
		A	B	C	D
1a	Analysis of requirements	++	++	++	++
1b	Generation and analysis of equivalence classes	+	++	++	++
1c	Analysis of boundary values	+	++	++	++
1d	Error guessing based on knowledge or experience	+	+	+	+

Analysis of the system and subsystems was performed, and analysis of the requirements to be entered at each stage was performed. Figure 4 is a functional analysis chart based on the component composition of

FCAS and it is composed so that the relationship of each function that constitutes the system can be grasped. Figure shows the software architecture for the FCAS, which allows the vehicle to be controlled by receiving information on the movement of the preceding vehicle. Each level of FTA was written in FMEA form as failure impact, failure type, and failure cause, and the results such as Figure 6 were drawn by filling out items of design verification. If the design management (verification) item of FMEA matches the TSR item, it is verified the requirement. It can confirm whether the TSR is properly derived, or it can satisfy ISO 26262 by confirming the linkage with the FSR by inversely deriving the TSR. The proposed system FMEA can identify more detailed risk factors for development systems through clear definitions of safety requirements and functions. Based on the proposed process, the effectiveness of the methodology was confirmed by conducting comparative analysis with existing FMEA.

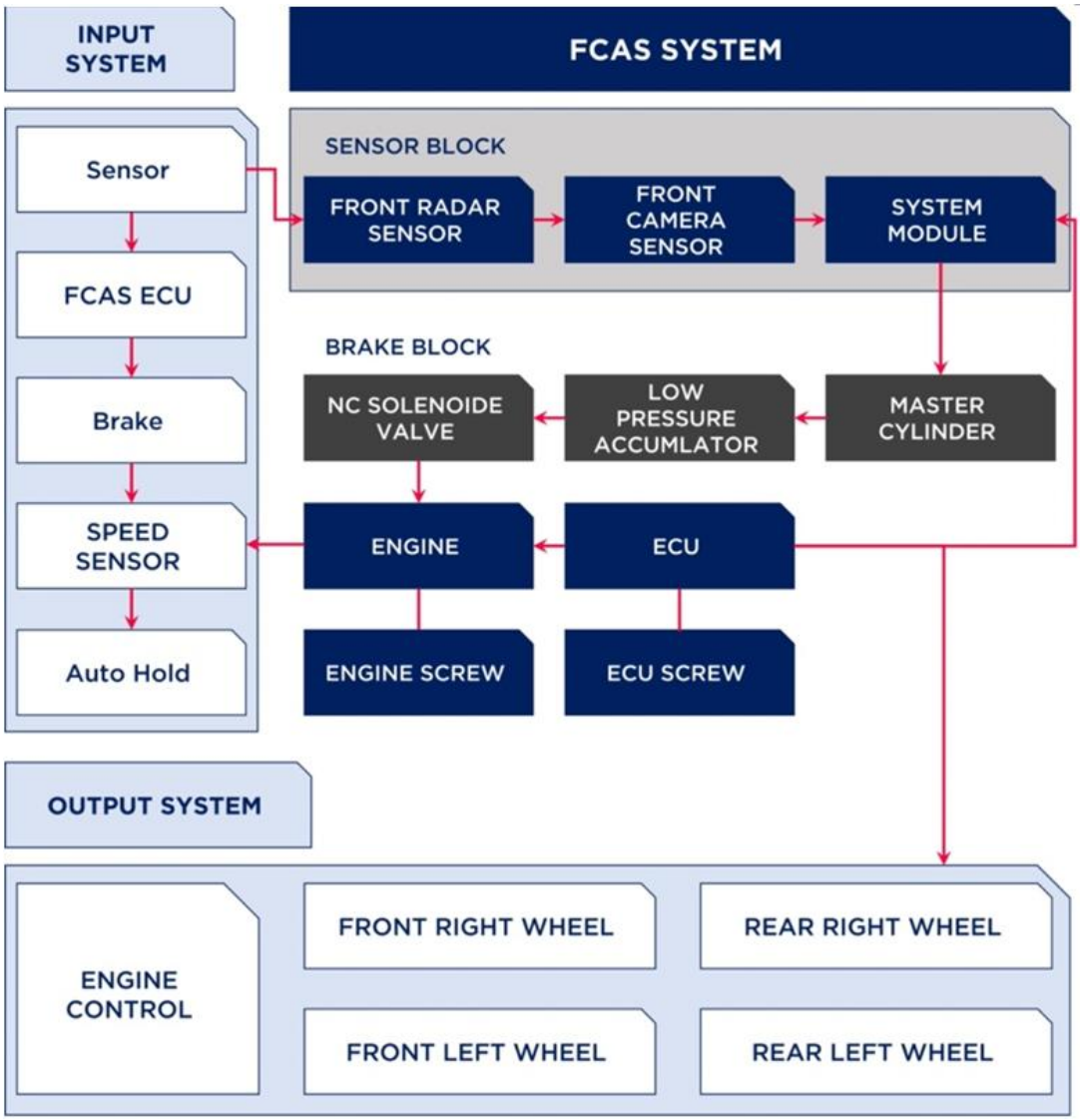

Figure 4. Hardware diagram of FCAS module assembly

Figure 5 shows a flow chart for the FCAS software architecture. As shown in Figure 5, FCAS detects vehicles and obstacles in front, reduces the speed if they are within the allowable safety distance range, and otherwise executes a command to stop the vehicle.

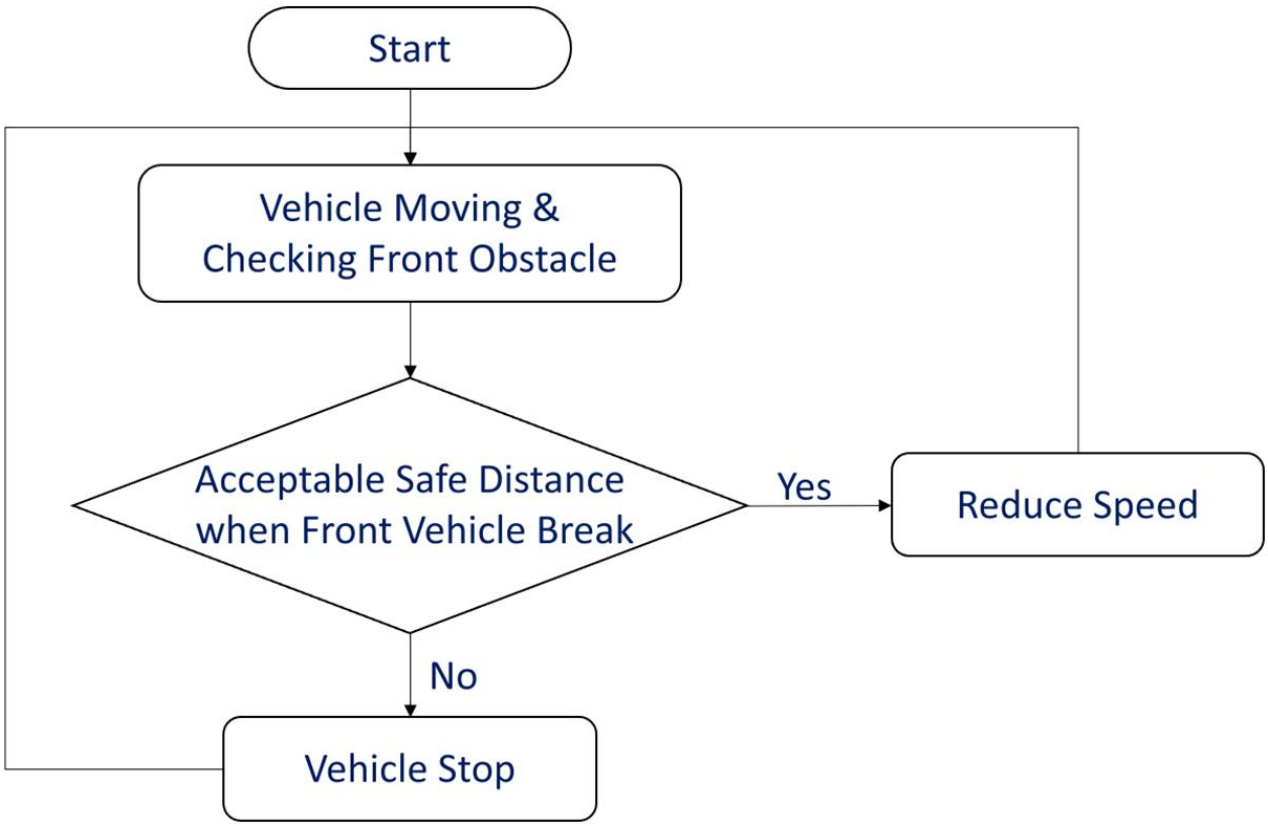

Figure 5. Data flow diagram of FCAS software architecture

The proposed system FMEA method has better results in identifying the risk factors for the development target than the existing FMEA method. The results of this study can be confirmed through Figure 6 and Figure 7. The proposed system FMEA has been identified as better identifying the risk factors that may occur in the target system. The results of the study confirmed that the ambiguity of performance methodology not included in the contents of the standard can reduce the possibility of engineering-independent activities.

FAILURE MODE and EFFECT ANALYSIS (FMEA)							
SYSTEM	FCAS(Forward Collision Avoidance Assist System)						
SUBSYSTEM	AEB (AUTONOMOUS EMERGENCY VEHICLE)		DESIGN MANAGER		-		
MODEL	-		TEAM		-		
FUNCTION	FAILURE MODE	FAILURE EFFECT	SEVERITY	CHARACTERISTICS	FAILURE CAUSE	OCCURENCE	RECOMMENDED ACTION
FRONT OBSTACLE DETECTION	Forward Obstacle Detection Unable	Collision with Front Obstacle	-	-	the obstacle sensing impossible due to the sensor malfunction	-	Sensor Performance Secured / Component Durability Secured
WHEEL BRAKING	Deceleration Unable		-	-	the deceleration impossible due to the brake part fault	-	Component durability secure
	Deceleration Late		-	-	deceleration degradation due to brake abnormality	-	Component Durability Secure
BRAKE HOLD	Vehicle Stop Unable	Secondary Accident Occurrence	-	-	Brake fixing device failure	-	Enhance Durability and Enhance Performance of Parts
			-	-	Fixability Decreased by Brake Wear	-	The Durability of Component and Abrasion Resistance Secure
ESC CONTROL	Electronic Stability Control Unable		-	-	Uncontrollable due to ESC mainboard fixation	-	Securing Board Performance / Securing Component Durability

Figure 6. FCAS's existing FMEA

POTENTIAL FAILURE MODE and EFFECT ANALYSIS (SYSTEM FMEA)							
SYSTEM	FCAS(Forward Collision Avoidance Assist System)						
SUBSYSTEM	AEB (AUTONOMOUS EMERGENCY VEHICLE)		DESIGN MANAGER		-		
MODEL	-		TEAM		-		
FUNCTION	FAILURE MODE	FAILURE EFFECT	SEVERITY	CHARACTERISTICS	FAILURE CAUSE	OCCURENCE	RECOMMENDED ACTION
FRONT OBSTACLE DETECTION	Forward Obstacle Detection Unable	Collision with Front Obstacle	-	-	The obstacle sensing impossible due to the sensor malfunction	-	Sensor Performance Secured / Component Durability Secured
			-	-	The obstacle sensing impossible due to the sensor signal failure	-	Sensor Control Board Performance and Durability Enhancement
WHEEL BRAKING	Deceleration Unable		-	-	The deceleration due to the brake signal control problem is not possible	-	Enhance Durability and Enhance Performance of Parts
			-	-	The deceleration impossible due to the brake part fault	-	Component durability secure
	Deceleration Late		-	-	Deceleration Decreasing due to Decreasing Obstacle Detection Performance	-	Obstacle Detection Performance Enhancement
			-	-	Deceleration degradation due to brake abnormality	-	Component Durability Secure
BRAKE HOLD	Vehicle Stop Unable	Secondary Accident Occurrence	-	-	Brake fixing device failure	-	Enhance Durability and Enhance Performance of Parts
			-	-	Fixability Decreased by Brake Wear	-	The Durability of Component and Abrasion Resistance Secure
ESC CONTROL	Electronic Stability Control Unable		-	-	Uncontrollable due to signal control system abnormality	-	Enhance Signal Control Performance and Secure Durability
			-	-	Uncontrollable due to ESC mainboard fixation	-	Securing Board Performance / Securing Component Durability

Figure 7. FCAS's system FMEA

5. Conclusion

The ISO 26262 standard describes only the necessary safety activities and requirements for how to perform in order to secure product safety during product development. This does not clearly express specific design methods, hardware, and software development methods, so guidelines for safety-secure vehicle development are essential. We presented development guidelines applying system engineering to clarify the definition of failure, which is the core content of ISO 26262. In the development process based on ISO 26262, we proposed to achieve more development goals and safety. We studied the methodology with the presentation of the process, explained the detailed execution method, and presented a verification case based on the actual function.

It is necessary to apply the method of deriving and verifying the failure which is the core to be performed for the functional safety of the potential failure in the process of ISO 26262. Especially, it is important to analyze E/E related parts and to draw requirements for those who need functional safety related to advanced driver assistance functions. Therefore, the usefulness of this study is in the functional safety target parts used together with machines and electronic components. It is necessary to conduct research on the part that needs driver assistance function and autonomous driving related function in practical terms. In the future, we will contribute to the effective performance of ISO 26262 functional safety by conducting detailed research on the risks caused by existing risks and system errors inherent in the operating environment of ISO 26262 functional safety.

Acknowledgement

This work was supported by a grant from R&D program of the Korea Evaluation Institute of Industrial Technology (20014470)

References

[1] R. E. Cole, “What really happened to Toyota?,” MIT Sloan Management Review. Vol. 52, No. 4, pp. 29, 2011.

[2] V. A. Banks, K. L. Plant, and N. A. Stanton, “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*. Vol. 108, pp. 278-285, 2016.
DOI: https://doi.org/10.1016/j.ssci.2017.12.023

[3] G. D. Jenssen, T. Moen, and S. O. Johnsen, “Accidents with Automated Vehicles-Do self-driving cars need a better sense of self?,” In *Proceedings of the 26th ITS World Congress*, Singapore, pp. 21-25, Oct. 21-25, 2019.

[4] B. Sari, “Fail-operational Safety Architecture for ADAS/AD Systems. In Fail-operational Safety Architecture for ADAS/AD Systems and a Model-driven Approach for Dependent Failure Analysis,” *Springer Vieweg*, Wiesbaden, pp. 31-75, 2020.
DOI: https://doi.org/10.1007/978-3-658-29422-9_3

[5] C. Webber, “Automotive Semiconductor Demand Forecast,” *Strategy Analytics*, 2013.

[6] ISO, “ISO 26262 : Road Vehicles –Functional Safety,” 2011.

[7] B. Kaiser, "Approaches towards reusable safety concepts," in *Proc. VDA Automotive SYS Conference*, 2012.

[8] S. H. Jeon, J. H. Cho, Y. Jung, S. Park, and T. M. Han, “Automotive hardware development according to ISO 26262,” In *13th international conference on advanced communication technology (ICACT2011) IEEE*. pp. 588-592, Feb. 13-16, 2011.

[9] Y. Luo, A. K. Saberi, and M. V. den Brand, “Safety-driven development and iso 26262. In: Automotive Systems and Software Engineering,” *Springer*, Cham, pp. 225-254, 2019.
DOI: https://doi.org/10.1007/978-3-030-12157-0_10

[10] A. Hycham, B. Mohamed, A. Morayo, and S. Emilia, “An integrated approach to implement system engineering and safety engineering processes: SASHA Project,” *ERTS2012*, pp. 1-6, 2012.
[11] A. Maftei, A. I. Dontu, and Barsanescu. “Applying FMEA methodology to evaluate different shapes of car struts,” In *IOP Conference Series: Materials Science and Engineering*, Vol. 997, No. 1, pp. 012120, 2020.
DOI: https://doi.org/10.1088/1757-899X/997/1/012120
[12] J. Choi, Y. Kim, J. Cho, and Y. Choi, “The Software FMEA Guideline for Vehicle Safety,” *Journal of Korea Multimedia Society*, Vol. 21, No. 9, pp. 1099-1109, 2018.
DOI: https://doi.org/10.9717/kmms.2018.21.9.1099
[13] J. Dawson, and D. Garikapati, “Extending ISO26262 to an Operationally Complex System,” In *2021 IEEE International Systems Conference (SysCon)*, pp. 1-7, 2021.
DOI: https://doi.org/10.1109/SysCon48628.2021.9447146
[14] S. I. Yang, and N. H. Lee, “The case study of ISO26262 product requirements analysis applying requirements engineering,” *KASE Conference, KASE*, pp. 2609-2615, 2012.
[15] D.G. Ahn, and J.H. Choi, and J.S. Jang, "How to perform FMEA effectively", *International Journal of Reliability and Applications*, Vol. 21, No. 2, pp. 131-143, 2021.
DOI: https://doi.org/10.33162/JAR.2021.6.21.2.131
[16] S. Y. Kim, H. G. Kim, and W. Y. Yun, “Reestablishment of RPN Evaluation Method in FMEA Procedure for Motors in Household Appliances,”, *KSQM, KISTI*, Vol. 35, No.1, pp. 1-9, 2007.
[17] Y. H. Kim, S. Y. Cho, and H. W. Kim, “A method of system requirements specification corresponding to ISO26262 functional safety,” *KASE Conference, KASE*, pp. 1548-1553, 2011.
[18] E. Armengaud, Q. Bourrouilh, G. Griessnig, H. Martin, and P. Reichenpfader, "Using the CESAR Safety Framework for Functional Safety Management in the context of ISO 26262," In *Embedded Real Time Software and Systems (ERTS2012)*, 2012.
[19] M. Ellims, H. Monkhouse, and A. Lyon, “ISO 26262: Experience applying Part 3 to an in-wheel electric motor,” In *Proc. 2011 6th IET International Conference on System Safety*, pp. 1-8, 2011.
DOI: https://doi.org/10.1049/cp.2011.0250
[20] M. Ringdofer, G. Griessnig, P. Draxler, and A. Schnellbach, “A systematical approach for "system item integration and testing" in context of ISO 26262,” *European Conference on Software Process Improvement*, Springer Cham, pp. 555-567, Sep. 9-11, 2020.
DOI: https://doi.org/10.1007/978-3-030-56441-4_42
[21] Y. Luo, A. K. Saberi, and M. V. den Brand, “Safety-Driven Development and ISO 26262,” In *Automotive Systems and Software Engineering*, Springer Cham, pp. 225-254, 2019.
DOI: https://doi.org/10.1007/978-3-030-12157-0_10
[22] S. Pasagadugula, G. Verma, and J. Harmalkar, “Effective Approach for Redundancy in Compliance with ISO 26262,” In *International Conference on Advances in Computing and Communication Engineering IEEE*, pp. 1-4, 2019.
DOI: https://doi.org/10.1109/ICACCE46606.2019.9079978
[23] M. A. Gosavi, B. B. Rhoades, and J. M. Conrad, “Application of Functional Safety in Autonomous Vehicles using ISO 26262 Standard:A Survey,” In *SoutheastCon IEEE*, pp. 1-6, 2018.
DOI: https://doi.org/10.1109/SECON.2018.8479057
[24] F. A. Da Silva, A. C. Bagbaba, S. Hamdioui, and C. Sauer, “Efficient methodology for ISO26262 functional safety verification,” In *2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, pp. 255-256, 2019.
DOI: https://doi.org/10.1109/IOLTS.2019.8854449