https://doi.org/10.21289/KSIC.2023.26.2.239

EPLA(Electric Park Lock Actuator) System Safety Design Based on Vehicle Functional Safety Standard ISO 26262

Eun-Hye Shin[1], Hyun-Hee Kim[2], Kyung-Chang Lee[3*]

〈Abstract〉

In this paper, we conduct a study on the design that can secure the safety of the EPLA system by performing safety activities based on the ISO 26262 standard for vehicle functional safety. In the case of a company developing a detailed system, it is responsible for verification through hardware design and safety analysis in the overall flow of safety activities, and safety analysis according to the ASIL safety level must be properly performed. At this time, there are cases where the safety goal quantitative metric value suggested by the ISO 26262 standard cannot be satisfied only by the hardware design of the basic function, so it is necessary to design and install the safety mechanism. Based on ISO 26262 safety activities, it is possible to derive an effective design plan through hardware safety analysis.

Keywords : ISO 26262, Vehicle Functional Safety, Electric Park Lock Actuator, Safety Analysis, Safety Design

1 Main Author, Futronic. Co., LTD.
E-mail: ehshin@futronic.co.kr
2 Co-Author, Pukyung National University, Research Professor
E-mail: hhkim@pknu.ac.kr
3* Corresponding Author, Major of Control & Instrumentation Engineering, Pukyung National University, Professor
E-mail: gclee@pknu.ac.kr

1. Introduction

Advanced electric/electronic(E/E) devices are rapidly increasing to implement various functions in vehicles. As the complexity of the devices installed in vehicles increases, the possibility of errors also increases, making it very important to ensure the safety of the system.

As the number and complexity of electronic control systems used in vehicle control increases, it has become necessary to require new technological paradigms for safety, as the reliability of component-level alone cannot guarantee vehicle safety. This led to the development of the ISO 26262 international standard for functional safety of electrical/ electronic systems installed in vehicles, aiming to reduce the occurrence of car accidents caused by errors in E/E systems[1-2].

ISO 26262 provides functional safety guidelines for the entire process from system design to verification, production, and disposal to reduce faults in electrical/electronic systems in vehicles. It also proposes that safety activities be performed according to the ASIL(Automotive Software Integrity Level) based on vehicle safety integrity levels.

ISO 26262 is a standard that applies the concept of functional safety(which has been utilized in the general industry through the IEC 61508 standard) to the automotive field. It has evolved into a new theory and practice of functional safety, which includes system design that focuses on hardware, software, and their integration, unlike the past safety concept that focused on the reliability of machine parts and electronic components.

This paper aims to propose a hardware system safety design that meets safety objectives through safety analysis based on the ISO 26262 functional safety standard for the EPLA(Electric Park Lock Actuator) system, a detailed system of the EPL(Electric Park Lock) system that provides electric parking lock function mounted on commercial vehicles such as trucks.

This paper is organized into five chapters. chapter 2 provides an overview of the ISO 26262 standard, while chapter 3 performs safety analysis and quantitative evaluation of the proposed EPLA system. Based on the safety analysis and quantitative evaluation, chapter 4 proposes a design approach for a hardware system that meets safety objectives. Finally, chapter 5 concludes the paper.

2. ISO 26262 Standard Overview

ISO 26262 is an international standard for ensuring the functional safety of E/E systems in the automotive industry. This standard provides a consistent approach to the design, development, verification, operation, and maintenance of software and hardware to ensure vehicle safety. ISO 26262 presents safety requirements for automotive E/E systems classified by ASIL and specifies safety activities applicable to each ASIL. The 2018 2nd

edition of ISO 26262 consists of 12 parts as shown in Fig. 1, and provides safety evaluation methodologies and tools applicable throughout the V-model development process[3-4].

In the item definition phase, the basic product functions and constraints, as well as items related to malfunctions of the functions, are described. Hazard analysis and risk assessment (HARA) involves analyzing hazardous events that may occur due to malfunctions of the system and deriving the ASIL and safety goals through risk assessment of the situation. Here, the item refers to a system or combination of systems that perform a function at the automotive level where ISO 26262 is applied. The system is a collection of elements, consisting of at least one sensor, controller, and actuator.

In the hazardous event classification phase, severity(S), probability of exposure(E), and controllability(C) are assigned to each identified hazardous event. The assigned levels are classified into S0 to S3 for severity, E0 to E4 for probability of exposure, and Co to C3 for controllability, as shown in Table 1. Based on the severity, probability of exposure, and controllability determined in the previous phase, the ASIL is determined, and safety goals are established. ASIL levels are divided into A, B, C, and D, with D being the

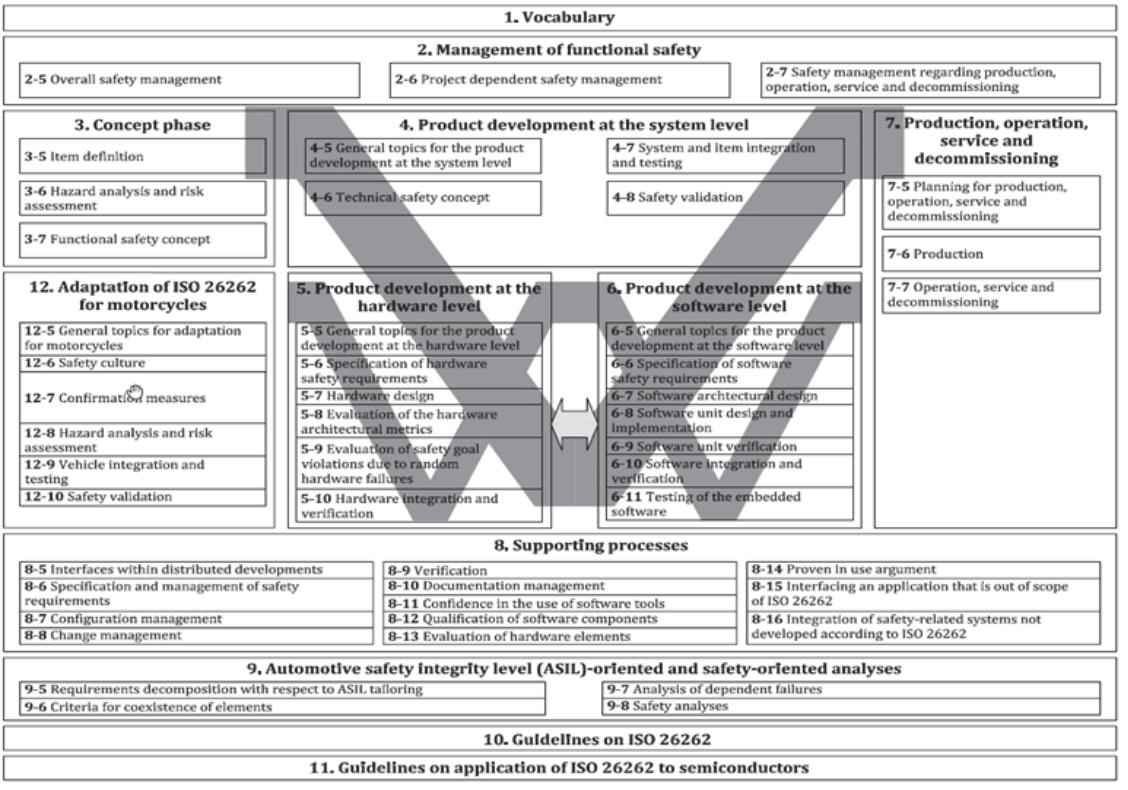

Fig. 1 Overview of the ISO 26262 series of standards

Table 1. Description of ASIL classification criteria

Factor	Classification of hazardous events				
Severity	S0	S1	S2	S3	
	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries	
Probability of exposure	E0	E1	E2	E3	E4
	Incredible	Very low probability	Low probability	Medium probability	High probability
Controllability	C0	C1	C2	C3	
	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable	

Table 2. Matrix for ASIL decision

Severity	Exposure	Controllability		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	QM
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

highest level. The higher the ASIL level, the higher the recommended requirements and level of safety activities[5].

Table 2 shows the criteria for determining ASIL levels based on combinations of the three elements of risk classification. The ASIL levels are divided into A, B, C, and D, with D being the highest level. The higher the level, the higher the recommended requirements and level of safety activities required.

The functional safety concept stage describes the information necessary to achieve safety objectives, such as safe state, functional safety requirements, and ASIL allocation relationships between architecture elements. In the technical safety concept stage, the safety ASIL allocation relationship between technical safety requirements and system elements required to achieve functional safety requirements is described. The system, HW, SW development stage proceeds with the development of hardware and software, reflecting non-functional requirements derived from the technical safety concept into functional requirements. Once development is complete, the functionality is tested by integrating the developed components. The safety analysis stage is a safety analysis technique for verifying safety activities in safety management, including FME(D)A and FTA.

3. EPLA System Safety Analysis

The vehicle EPL(Electric Park Lock) system

is a device that provides electric parking locking. It is installed in conventional or electric vehicle transmissions to prevent unintended vehicle rollback when the vehicle is stopped.

Fig. 2 is a conceptual diagram of the EPL system. When deriving a system design through safety analysis, the system referred to is the EPLA system, which is a detailed system of the EPL system and is indicated by the red highlighted part in the diagram. The control axis of the EPL actuator system is the output shaft that reaches the gearbox, and it is connected to the EPL actuator via a spline connection.

In this paper, the design of the EPL system is carsried out while ensuring system safety based on the vehicle function safety activity process according to the ISO 26262 standard. Through hazard analysis and risk assessment (HARA), the identified EPLA system function and ASIL rating were used to derive safety goals. Although a total of six safety goals were derived through HARA analysis, only safety goal items that are assigned ASIL based on the ISO 26262 functional safety standard need to be considered as the criteria for performing safety activities in the system design based on safety analysis. Therefore, the ASIL C level, the highest assigned ASIL level, was selected as the safety goal to consider for the system design.

Table 3 shows the details of safety goals classified according to the ASIL C level determined through HARA analysis. Safety analysis should be performed in accordance with the safety goal metric criteria shown in

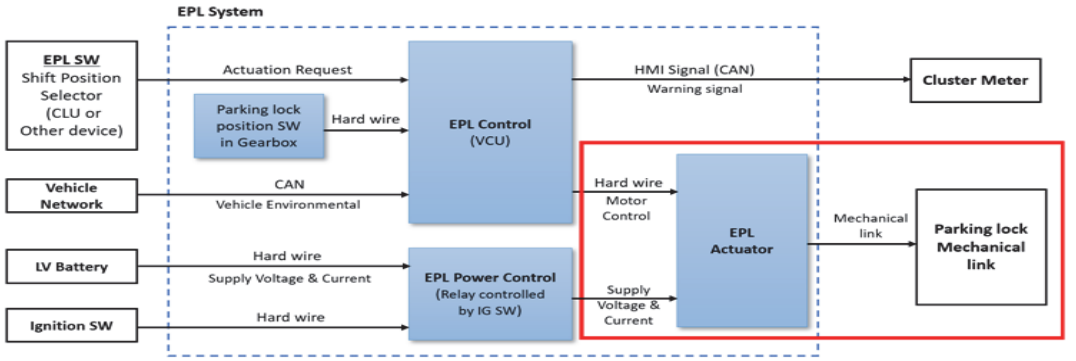

Fig. 2 Electric park lock system

Table. 3 Safety goal

ID	Safety goal	Safe state	Single-point fault metric	ASIL
	Description	PMHF target value	Latent fault metric	
G006	Avoidance of unintended release of EPL while the vehicle is at standstill	EPL locked	≥ 97 %	C
	When park locked, the lock must not be unlocked without the driver's intention.	$< 10^{-7}$ /h	≥ 80 %	

the figure to ensure that the safety analysis results meet the requirements while designing the system.

Fig. 3 represents the technical safety requirements of the EPLA system. Based on the safety goals of the EPLA system, functional safety requirements are defined and the technical safety requirements are defined to implement them. In this paper, only ensuring the operational integrity of the EPLA system was set as the top-level technical safety requirement, and the requirements for implementation and ensuring safety were detailed as sub-level technical safety requirements and were analyzed accordingly.

Fig. 4 represents the hardware safety requirements of the EPLA system. As the safety

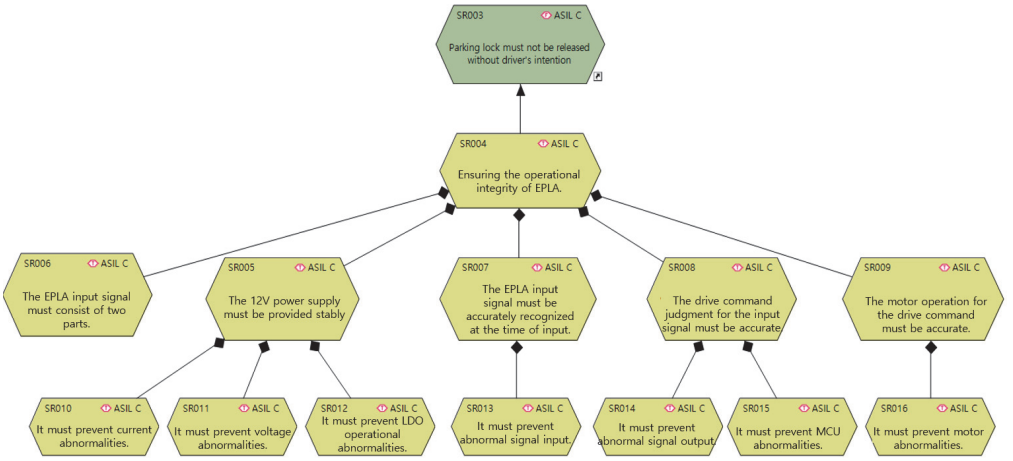

Fig. 3 Technical safety requirements for EPLA system

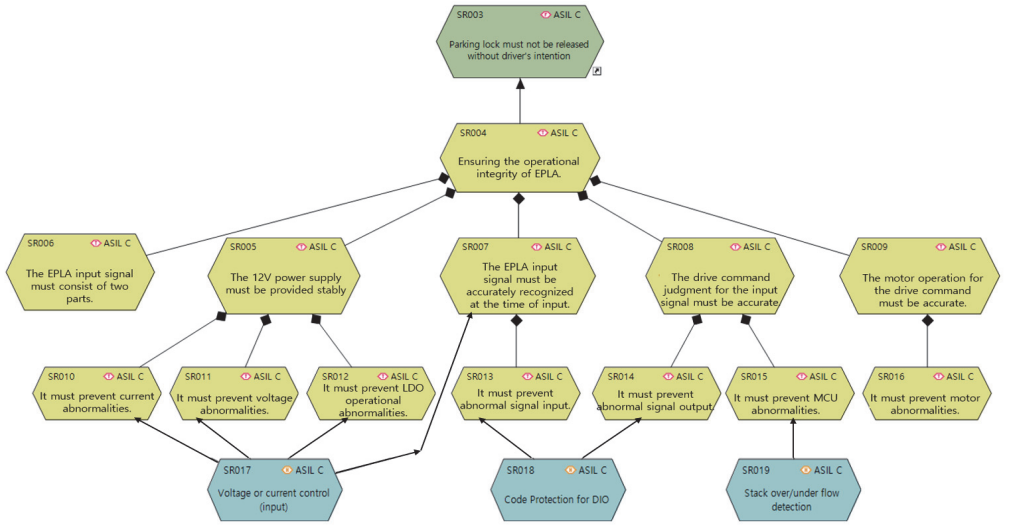

Fig. 4 Hardware safety requirements for EPLA system

mechanisms derived from safety analysis should be reflected in the hardware safety requirements without reflecting the detailed requirements for hardware implementation, the relevant contents have been applied. The development of function, technology, hardware, software requirements requires defining the scope of the concept and developing compliance standards accordingly, based on the development methods and development management, operational guidelines. Therefore, active agreement and discussion are necessary within the organization performing safety activities.

The types of safety mechanisms that affect quantitative analysis were selected based on the safety mechanisms listed in annex D of ISO 26262. In the current system elements of the development system, the safety mechanism application function blocks were categorized into power supply, analogue and digital I/O, processing unit(MCU), and actuators. The diagnostic coverage(DC) of the safety mechanism is 60% for the low level, 90% for the medium level, and up to 99% for the high level. While using safety mechanisms with high diagnostic coverage may seem advantageous from a safety standpoint, the selection of which safety mechanism to apply should be based not only on diagnostic coverage, but also on implementation and applicability. Therefore, a judgment must be made on which safety mechanism to apply.

Table 4 shows the safety mechanisms for each level of diagnostic coverage that will be applied to the system system elements. Safety analysis was conducted to determine which safety mechanisms to apply, considering factors such as ease of development, implementation speed, and flexibility in system integration.

By combining safety mechanisms for each diagnostic coverage (DC) level of each function block, a maximum of 144 safety analysis cases can be generated. In this paper, we plan to conduct safety analysis simulations to determine the optimal selection of safety mechanisms to ensure hardware safety.

4. EPLA System Design

Based on the ISO 26262 standard for vehicle functional safety, safety activities were performed and various safety mechanisms were reviewed to ensure the safety of the identified functional blocks in order to achieve safety goals. Through safety analysis, a total of 144 design cases were generated for the combination of safety mechanisms that could be implemented according to certain criteria and methods in a system designed with basic functions.

Table 5 represents the results of the design obtained by dividing the safety goals priority and safety analysis case generation through the EPLA system safety analysis. First, a sequential combination of safety mechanisms for safety analysis was carried out, starting from applying safety mechanisms with lower diagnostic coverage to higher diagnostic

Table 4. Safety mechanism for system elements

Element	Safety mechanism /Measure	Typical diagnostic coverage	Aim
Power supply	Voltage or current control (output)	High	To detect as soon as possible wrong behavior of output current or voltage values
	Voltage or current control (input)	Low	To detect as soon as possible wrong behavior of input current or voltage values
Analogue and digital I/O	Multi-channel parallel output	High	To detect random hardware failures(stuck-at failures), failures caused by external influences, timing failures, addressing failures, drift failures, and transient failures
	Code protection for digital I/O	Medium	To detect random hardware and systematic failures in the input/output dataflow
	Failure detection by on-line monitoring	Low	To detect failures by monitor -ing the behavior of the system in response to the normal (on-line) operation
Processing units (MCU)	HW redundancy (e.g. dual core lockstep, asymmetric redundancy, coded processing)	High	To detect, as early as possible, failures in the processing unit, by step-by-step comparison of internal or external results or both produced by two process -ing units operating in lockstep
	Self-test supported by hardware (one-channel)	Medium	To detect, as early as possible, failures in the processing unit consisting of physical storage and functional units
	Stack over/under flow detection	Low	To detect, as early as possible, stack over or under flows
Actuators (motor)	Monitoring (i.e. coherence control)	High	To detect the incorrect operation of an actuator
	Failure detection by on-line monitoring	Low	To detect failures by monitoring the behavior of the system in response to the normal (on-line) operation

Table 5. Design proposal with system analysis

No	Design plan	Safety analysis case	Advantages	Disadvantage
1	System design plan according to safety analysis case safety mechanism combination sequence	67	An easy way to approach safety analysis without a strategy	Due to the premise of safety analysis for all conditions, there is a time constraint in deriving the design proposal.
2	Safety analysis result priority system design	76[1)]	Among the conditions for achieving safety goals, it is possible to achieve the conditions for minimizing safety violations	Inadequate consideration of cost or design infrastructure (development time and manpower availability, optimization implementation method, etc.)
		144[2)]		

[1)] Analysis priority: SPFM 〉 LFM 〉 PMHF
[2)] Analysis priority: PMHF 〉 SPFM 〉 LFM

coverage. ASIL C safety goals were achieved in the 67th safety analysis case. In this case, the power function block was equipped with a low diagnostic coverage safety mechanism, the IO function block with a low diagnostic coverage safety mechanism, the MCU function block with a Medium diagnostic coverage safety mechanism, and the Motor function block was not equipped with a safety mechanism.

According to the safety analysis, the system design can be derived based on the priority of safety objectives, and it was confirmed in the 76th safety analysis case. In this case, the safety mechanisms can be configured with low diagnostic coverage safety mechanism for the power function block, Medium diagnostic coverage safety mechanism for the IO function block, low diagnostic coverage safety mechanism for the MCU function block, and no safety mechanism for the Motor function block.

5. Conclusion

This paper presents a study on the design of the EPLA system with the aim of ensuring its safety by performing safety activities based on the vehicle functional safety standard ISO 26262. To achieve this, safety mechanisms were incorporated into the EPLA system, and a safety analysis simulation was conducted to select safety mechanisms with different diagnostic coverage for each system component as prescribed by the ISO 26262 standard to ensure safety. A total of 144 safety analysis cases were examined, of which 48 valid cases were identified that satisfied the safety objectives by incorporating appropriate safety mechanisms. Among them, the 76th safety analysis case was proposed as the EPLA system design with the highest priority for safety objectives. Further research is planned to be conducted on the detailed implementation of the system and proposal of design plans.

Acknowledgements

This research was financially supported by the Ministry of Trade, Industry and Energy (MOTIE) and Korea Institute for Advancement of Technology(KIAT) throughthe export-linked automotive parts technology development program(PP0020927_Development of an efficiency improvement actuator equipped with a magnetic sensing function for safety transmission for wheel drive conversion).

References

[1] ISO 26262:2011 Road vehicle - Functional safety, Part 1~10, ISO(International Organization for Standardization), (2011).
[2] IEC 61508:2010 Functional safety of electrical/ electronics/programmable electronics safety-related systems - Part. 1~7, ISO(International Organization for Standardization), (2010).
[3] ISO 26262:2018 Road vehicle - Functional safety, Part 1~12, ISO(International Organization

for Standardization), (2018).
[4] Technical Report, IEC TR 62380-Reliability data handbook 1st Ed, IEC, (2004).
[5] B.C.Kim, "Automotive Functional Safety ISO 26262 Standard and the Response of the Automotive Industry," The journal of Korea Institute of Electronics Engineers, V.40 No.5, pp. 20-33, (2013).

(Manuscript received March 13, 2023;
revised April 2, 2023; accepted April 10, 2023)