International Journal of Internet, Broadcasting and Communication Vol.13 No.3 169-177 (2021)
http://dx.doi.org/10.7236/IJIBC.2021.13.3.169

IJIBC 21-3-22

On the Ensuring Safety and Reliability through the Application of ISO/PAS 21448 Analysis and STPA Methodology to Autonomous Vehicle

Min Joong Kim*, Kyoung Lak Choi**, Joo Uk Kim***, Tong Hyun Kim****, Young Min Kim*****†

** Ph. D. Candidate, Department of Systems Engineering, Ajou University, Korea*
*** Senior Engineer, Automotive Engineering Service Team, DNV GL Business Assurance Korea, Korea*
**** Senior Researcher, Advanced Logistics System Research Department, Korea Railroad Research Institute, Korea*
***** CEO, CanLab Co., LTD. , Korea*
****** Associate professor, Department of Systems Engineering, Ajou University, Korea*
aquamjkim@ajou.ac.kr, kyoung.lak.choi@dnvgl.com, jookim@krri.re.kr, ken@can-lab.co.kr, pretty0m@ajou.ac.kr

Abstract

Recently, the use of electric and electronic control systems is increasing in the automobile industry. This increase in the electric and electronic control system greatly increases the complexity of designing a vehicle, which leads to an increase in the malfunction of the system, and a safety problem due to the malfunction is becoming an issue. Based on IEC 61508 relating to the functional safety of electrical/electronic/programmable electronics, the ISO 26262 standard specific to the automotive sector was first established in 2011, and a revision was published in 2018. Malfunctions due to system failure are covered by ISO 26262, but ISO/PAS 21448 is proposed to deal with unintended malfunctions caused by changes in the surrounding environment. ISO 26262 sets out safety-related requirements for the entire life cycle. Functional safety analysis includes FTA (Fault Tree Analysis), FMEA (Failure Mode and Effect Analysis), and HAZOP (Hazard and Operability). These analysis have limitations in dealing with failures or errors caused by complex interrelationships because it is assumed that a failure or error affecting the risk occurs by a specific component. In order to overcome this limitation, it is necessary to apply the STPA (System Theoretic Process Analysis) technique.

Keywords: *System Theoretic Process Analysis (STPA), ISO 21448, SOTIF, Autonomous vehicles, Safety Analysis, Hazards, Safety*

1. Introduction

Recently, the use of electric/electronic control systems is increasing not only in the automobile industry but also in various industries. The increase in the use of such electric/electronic control systems greatly increases the complexity of designing the system, which leads to an increase in system malfunctions, and social safety issues due to such malfunctions are becoming an issue.

Manuscript Received: July. 27, 2021 / Revised: August. 3, 2021 / Accepted: August. 6, 2021
Corresponding Author: pretty0m@ajou.ac.kr
Tel: +82-31-219-3949, Fax: +82-31-219-2334
Associate professor, Department of Systems Engineering, Ajou University, Korea

1.1 Background and necessity

An example of an accident caused by a malfunction is an accident with the radiation medical device Therac-25 in 1985, and the automobile industry is no exception. As in the case of Toyota accident in Japan in 2009, the software controlling the system became a problem and an accident occurred. In the automobile industry, the international standard for automotive functional safety "ISO 26262 – Road Vehicle – Functional Safety" was established in 2011 based on the IEC 61508 international standard, which is the functional safety of electric/electronic/programmable electronic safety management systems. Afterwards, the 2nd edition was distributed through revision and supplementation in 2018 [1]. The purpose of ISO 26262 is to prevent risks arising from defects in systems and components and to improve functional safety and reliability. However, dangerous situations can occur even when the system or component is not defective. For example, there are no defects in the camera sensor, but the recognition function may be lost due to sudden changes in illuminance. As a result, a malfunction may occur and an unintended risk may also exist. To solve this problem, a new functional safety standard called "ISO/PAS 21448 – SOTIF – Safety Of The Intended Functionality" was proposed [2].

ISO 26262 presents requirements related to safety throughout the entire life cycle. Representative risk analysis techniques include FTA (Fault Tree Analysis), FMEA (Failure Mode and Effect Analysis), and HAZOP (Hazard and Operability). This analysis method is a chain of event model, which is a theory that accidents occur due to consecutive errors of components [4]. These analysis techniques view the failure of a specific component as a risk. However, as the system becomes more complex in recent years, there is a limit to handling failures or errors due to component failure as well as complex interrelationships or external environmental factors [3, 5]. In order to deal with the errors caused by the interaction between modern complex systems, Leveson proposed the STPA (System Theoretic Process Analysis) method based on the STAMP (System Theoretic Accident Model and Processes) model [3]. The STPA technique identifies risks by identifying UCA (Unsafe Control Action) by the interaction of system components.

1.2 Definition of the problem

Chen L. et al. (2020) obtain a new method by combining STPA and FMEA [6]. However, combining the two analysis methods complicates the procedure and consumes a lot of analysis time. Abdulkhaleq, A. et al. (2017) was proposed that STPA approach as a risk analysis according to ISO 26262 [10]. It confirms that STPA is an effective and efficient approach for deriving safety constraints [10]. Ishimatsu, T. et al. (2010) evaluated the feasibility and usefulness of STPA for the initial system design phase [11]. It has problems with how to model and analyze systems.

For the scope and goal of this study, as shown in Figure 1, STPA was selected among the risk analysis methods. We analyze the feasibility of securing the reliability of STAP, and present examples of applications to the AEB(Automatic Emergency Braking) system to verify the efficiency of STPA, and confirm its feasibility.

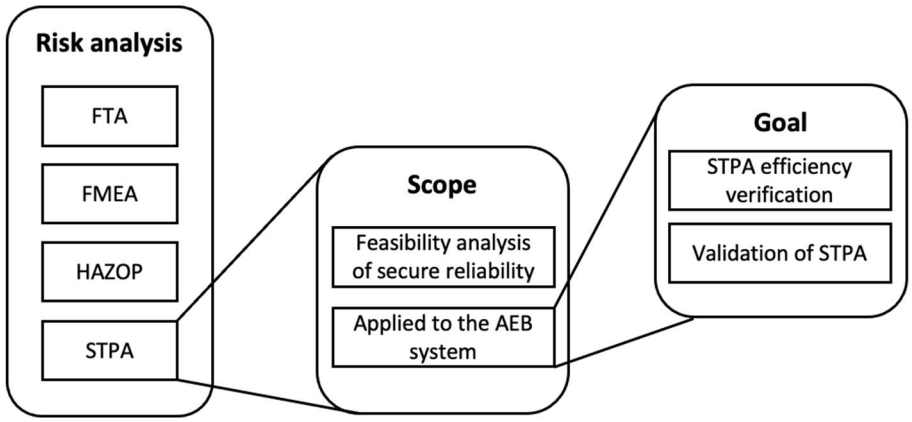


Figure 1. Scope and goal of this study

Figure 2 shows this study procedure. First, ISO 26262 and ISO/PAS 21448 (SOTIF) are described. In addition, the limitations of risk analysis such as FTA, FMEA, and HAZOP are described, and the necessity of STPA is described. And feasibility was confirmed by applying STPA to the automatic emergency braking (AEB) system.

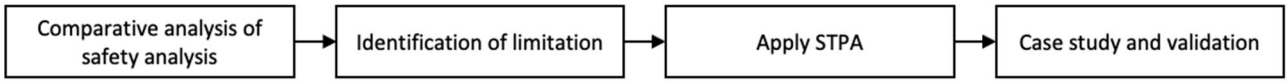


Figure 2. Procedure of this study

1.3 Composition of this paper

The composition of this paper is as follows. Section 2 describes the theoretical background. Through comparative risk analysis such as FTA, FMEA, and HAZOP, limitations are presented and the necessity of STPA is discussed. Section 3 explores the application of STPA to AEB systems. Finally, Section 4 describes the conclusions and limitations of this study and future works.

2. Feasibility analysis of methods for securing reliability based on ISO 26262 and STPA

2.1 Comparison between ISO 26262 and ISO/PAS 21448

ISO 26262 is an international standard for functional safety established by ISO to prevent accidents caused by functional safety system errors in electric and electronic systems in the automotive field. ISO 26262 presents safety-related requirements in the entire life cycle from development to production and disposal. The goal of ISO 26262 is a safety goal, and this safety goal has an ASIL (automotive safety integrity level), which is classified into QM, A, B, C, and D. After setting the safety goal, FMEA, FTA, HAZOP, etc. are used for safety analysis.

SOTIF deals with situations that are not failures. SOTIF is divided into four main areas. 1) Known safe scenarios (area1), 2) Known unsafe scenarios (area2), 3) Unknown safe scenarios (area4), and 4) Unknown unsafe scenarios (area3). Figure 1 shows a visualization of the four areas of SOTIF. The purpose of SOTIF is to reduce unknown or unsafe situations.

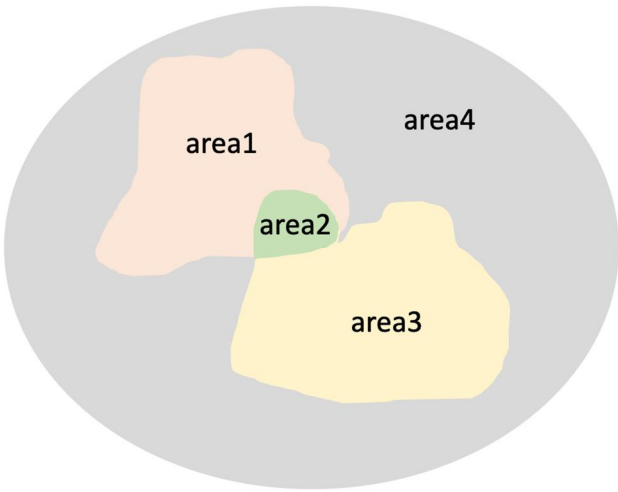


Figure 3. Visualization of the Known/Unknown and Safe/Unsafe Scenarios

2.2 Comparison of risk analysis method FTA, FMEA, and HAZOP

FTA is that finds the cause of a failure using a combination of logic gates. Failures and causes of failure are composed of trees, and the failure is located at the top of the tree, and the final cause of failure is located at the bottom (root). All causes can be expressed by various logical combinations, and the probability that a failure can occur is calculated as the final combination. Figure 4 shows the FTA implementation procedure.

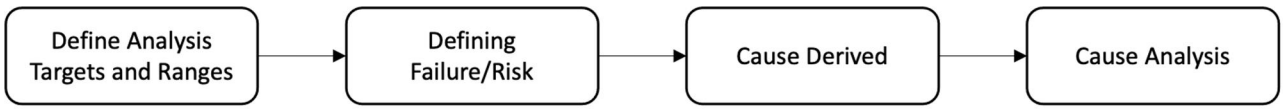


Figure 4. procedures of FTA

FMEA is a qualitative and inductive failure analysis technique, which is the most used and well-known technique in the field of reliability methodology. FMEA is a technique used to identify potential failure modes and causes for components of the system in the initial development process [6-7]. FMEA measures the severity, occurrence, and detection probability to compute the results of the identified failure modes [6]. Figure 5 shows the procedure for performing FMEA.

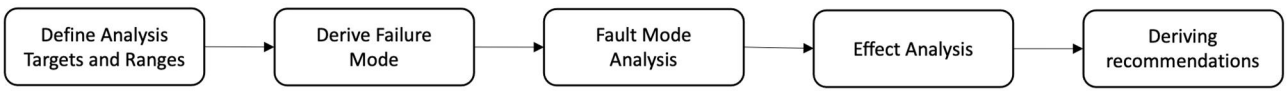


Figure 5. procedures of FMEA

HAZOP is a technique to derive all deviations of a system or process and analyze risks, a qualitative risk analysis technique for identifying whether deviations occur or occur due to deviations from the design intent [8]. HAZOP analyzes possible risks using guide words [9]. Figure 6 shows the procedure of HAZOP.

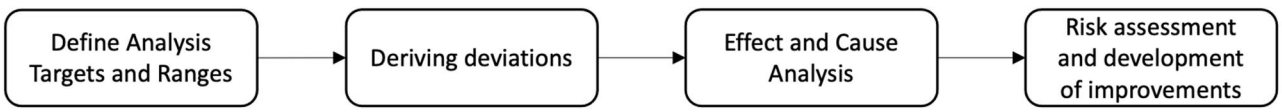
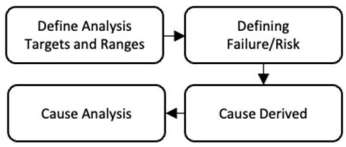
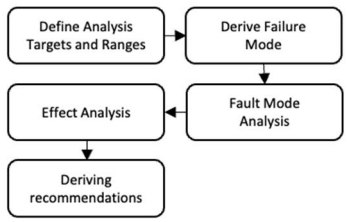
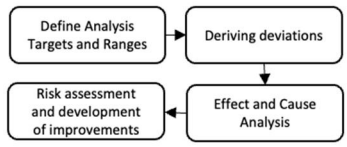


Figure 6. procedures of HAZOP

Table 1. Comparison of risk analysis

Item	FTA	FMEA	HAZOP
Concept	For predictable accidents, deductively review defects or errors that cause the accident and evaluate safety	Decrease the failure rate by defining the possible failure modes of the system and analyzing the effects and causes	Identification of predictable abnormal behavior from normal system operation using guide words
Purpose	Check for combinations of device failures and operator errors	Derive impact on the system Suggest failure reduction plan	Identify risks and problems
Procedure			
Characteristic	AND, OR tree structure	Review of improvement measures	Using guide words
Disadvantage	Spend a lot of time and money Expert required Prerequisite for securing failure rate	Reflecting the author's subjective opinions Difficult to reflex complex interactions	Requires a large number of team members Rely on expert experience Spend a lot of time

2.2 Procedures for performing STPA

FTA, an existing risk analysis method, requires specialized knowledge such as statistics and probability, and has limitations in that the larger the size of the analysis system, the larger it is, and it takes a lot of cost and time. FMEA has limitations in that it is difficult to consider complex interactions, and the subjective opinion of the author is reflected. In addition, since HAZOP analyzes using only guide words, it is dependent on the experience of experts, and has limitations in that it takes a lot of time and money. These risk analysis focuses on component failure.

With the recent increase in electrical and electronic control systems, the proportion of software increases and the system becomes more complex, making it difficult to analyze using the existing risk analysis methods [3, 5]. To overcome this point, Leveson presented the System Theoretic Accident Model and Process (STAMP) model based on systems theory [3, 5]. STPA (System Theoretic Process Analysis) is a STAMP-based risk analysis method that analyzes the system from a control point of view and identifies inappropriate controls that can cause risks. In addition to SW and HW, STPA has the advantage of analyzing risks by expressing all factors related to the development and operation of the system as a model, such as factors such as people and the environment. Figure 7 shows the STPA procedure, which is a STAMP-based risk analysis method.

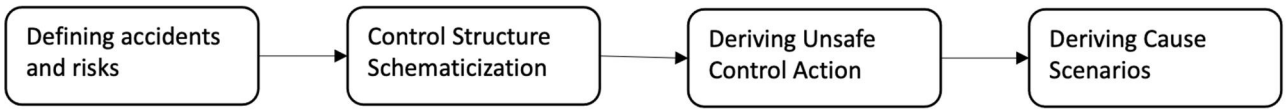


Figure 7. procedures of STPA

Phase 1 defines accidents and hazards. Definitions are again categorized into detailed steps such as defining thinking, defining system-level risk, and deriving system-level safety constraints. The accident definition phase defines the scope of the accident and gives an ID to facilitate tracking of the accident. In the system level risk definition, the target system is selected, the scope is defined, and the risk is defined. System-level safety constraint derivation derives a state or action to prevent the occurrence of the previously defined risk.

In phase 2, the Control Structure schematic consists of subjects, objects, controls, and responses from a control perspective.

In phase 3 UCA (Unsafe Control Actions) derivation, we analyze the risk by identifying the unstable control that can cause the risk of the system into four types, as shown in Table 2.

Table 2. Unsafe Control Structure that can cause a hazard

Type	Definition
Not Providing Causes Hazard	Risk arises from not providing control
Providing Causes Hazard	Risk arises by providing control
Too Late, Too Soon, Out of order	Provided control, but risked too late, too soon, or in the wrong order
Stopped Too Soon Applied Too Long	Ending control too early or giving too long a risk

In phase 4 cause scenario derivation, the causes of the 4 types of UCA derived above are analyzed. It can be largely classified into two types, and the first is to derive the cause of why it was provided insecurely. The second is to analyze the causes of improperly performed or not performed control. Finally, based on these causes, a cause scenario is created.

3. Scenario derivation by applying STPA to AEB system

The AEB (Autonomous Emergency Braking) system is an automatic emergency braking system that recognizes obstacles in front of a moving vehicle, anticipates a collision, and automatically operates the brake to prevent a collision. The operation sequence of the AEB system is as follows. 1) It receives target information through sensor information and detects obstacles ahead by fusion of information from ECU (Electric Control Unit). 2) Calculate TTC (time-to-collision) by calculating the relative speed and distance to the vehicle in front, based on the ego vehicle. 3) Control the movement so that the vehicle does not collide according to the calculated TTC value.

Defining phase 1 accidents and hazards results in the following: Accidents occur when an occupant is injured or killed while driving and the vehicle is damaged. A risk is when a passenger is in a dangerous situation while driving or does not maintain a minimum safe distance from the preceding vehicle.

Table 3. Definition of an accident

ID	accident
A1	Injuries or deaths of passengers while driving the car
A1-1	Collision with the car in front of you
A1-2	Collision with a sudden cut-in vehicle.
A2	Vehicle Damage

Table 4. Definition of risk

ID	Risk	Related accidents
H1	Passengers are in danger while driving	A1, A2
H2	The vehicle does not maintain a minimum safe distance from moving objects	A1, A2

The phase 2 control structure schematic is shown Figure 8. The information obtained from the sensor calculates the speed and distance and transmits the information, and based on this, a command is issued to the vehicle.

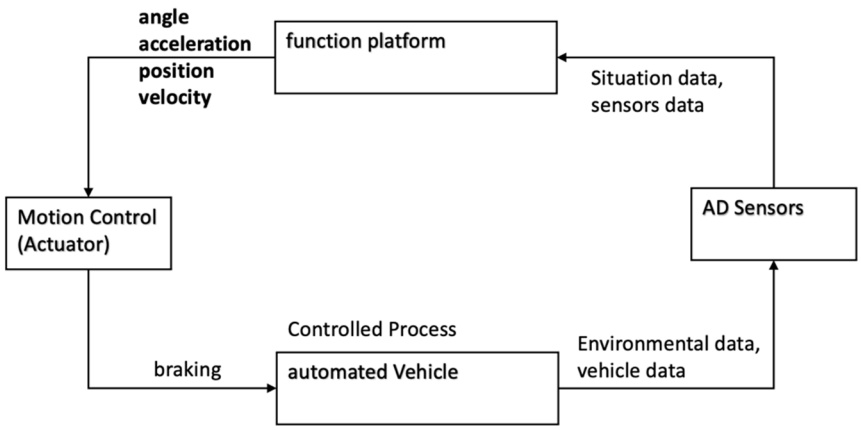


Figure 8. Control Structure of AEB System

Table 4 shows that the phase 3 Unsafe Control Action. This is a case in which a brake command is requested while driving but the brake command is not executed, or the brake command is requested too late.

Table 5. Definition of Risk

Control Action	Not Providing Cause Hazard	Providing Cause Hazard	Too Late, Too Soon, Out of order	Stopped Too Soon, Applied Too Long
Braking request	UCA1: Failure to execute brake command while driving	-	UCA2: Requesting a brake command too late	-

The phase 4 cause scenario is as follows. The cause of the UCA1 not performing the braking command while

driving may be incorrect provision of the vehicle's current position value or incorrect sensor measurement value. Alternatively, there may be a cause of not receiving the brake command itself. Possible causes for UCA2 are providing incorrect current position values of the car or incorrect sensor readings.

Table 6. Deriving causal scenarios for UCA

ID	causal scenarios
UCA1	UCA1-SE1. Incorrectly providing the car's current location value
	UCA1-SE2. Incorrectly giving measured sensor values
	UCA1-SE3. Failed to receive brake command
UCA2	UCA2-SE1. Incorrectly providing the car's current location value
	UCA2-SE2. Incorrectly giving measured sensor values

4. Conclusion

In the past, FTA, FMEA, HAZOP, etc. were utilized by focusing on specific components for the cause of accidents. However, as the utilization of software has increased recently, the system has become more complex. As a result, the risk of an unintended accident such as an external environment rather than a system or component error has increased. In addition, not only failures caused by components, but also causes due to interactions between components or systems have increased. Therefore, the ISO/PAS 21448 standard was established to prevent the risk of unintended accidents, and the STPA technique was developed to deal with failures or errors caused by the interaction of components.

In this paper, describes the necessity of ISO/PAS 201448 international standard and STAP analysis method. STPA analysis provides structured scenario analysis. In addition, among numerous systems of automobiles, STPA was applied to the AEB system, an emergency automatic control system, to analyze risks and derive a cause scenario. We confirmed that STPA was effective for the identification of hazards or risks. Objectivity will be secured by deriving scenarios using STPA for various systems in the future.

Acknowledgement

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

References

[1] ISO 26262 : Road Vehicles - Functional Safety, *International Organization for Standardization*, 2018.
[2] ISO/PAS 21448 - Road vehicles - Safety of the intended functionality, *International Organization for Standardization, 2019*
[3] Leveson, N., Engineering a safer world: Systems Thinking Applied to Safety *MIT Press*, 2011.
[4] Benner, L., Accident investigations: Multilinear events sequencing methods *Journal of Safety Research*, 1975.
[5] Leveson, N., "A New Accident Model for Engineering Safer systems, *Safety science*, 42(4), 237-270, 2004. DOI: https://doi.org/10.1016/S0925-7535(03)00047-X
[6] Chen, L., Jiao, J., and Zhao, T., A Novel Hazard Analysis and Risk Assessment Approach for Road Vehicle Functional Safety through Integrating STPA with FMEA. *Applied Sciences* 10.21: 7400, 2020. DOI: https://doi.org/10.3390/app10217400

[7] Standard, Military, MIL-STD-1629A: Procedures for Performing a Failure Mode, Effects and Criticality Analysis, *Department of Defense, Washington DC*, 1977.

[8] Redmill, F., Chudleigh, M., and Catmur, J. System safety: HAZOP and software HAZOP, *Chichester: Wiley*, 1999.

[9] Travassos, G., Shull, F., Fredericks, M., and Basili, V. R. Detecting defects in object-oriented designs: using reading techniques to increase software quality. *ACM sigplan notices*, 34(10), 47-56, 1999.
DOI: https://doi.org/10.1145/320385.320389

[10] Abdulkhaleq, A. Wanger, S., Lammering, D., Boehmert, H., and Blueher, P. Using STPA in compliance with ISO 26262 for developing a safe architecture for fully automated vehicles. *arXiv preprint arXiv:1703.03657,* 2017.

[11] Ishimatsu, T., Leveson, N. G., Thomas, J., Katahira, M., Miyamoto, Y., and Nakao, H., Modeling and hazard analysis using STPA, 2010.

[12] Xia, L., Chung, T. D., and Kassim, K. A. A., An automobile detection algorithm development for automated emergency braking system, *2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 2014.
DOI: https://doi.org/10.1145/2593069.2593083

[13] Diederichs, F., Schüttke, T., and Spath. D., Driver intention algorithm for pedestrian protection and automated emergency braking systems, *2015 IEEE 18th International Conference on Intelligent Transportation Systems*. IEEE, 2015.
DOI: https://doi.org/10.1109/ITSC.2015.174