On ISO 26262 Compliance and Safety Assurance for Autonomous Vehicles using STPA

ISO 26262 Compliance and Safety Assurance using STPA

Changsheng Gao [a], Xuezhu Yang [b], Chengrui Sun [c*]

Intelligent Connected Vehicle Development Institute, FAW, Changchun, China

[a]gaochangsheng@faw.com.cn
[b]yangxuezhu@faw.com.cn
[c*]sunchengrui@faw.com.cn

Abstract. Recently, the use of electrical and electronic control systems has been increasing in various industries. In particular, in the automobile industry, unlike mechanical vehicles in the past, today's vehicles have a significant increase in complexity as the system of the electronic control device increases, and accordingly, the overall system malfunction increases. Although IEC 61505, a functional safety specification for electrical / electronic / programmable electronic safety management systems across industries, does not reflect the specificity of the automotive field. Therefore, ISO 26262, an international standard for automotive functional safety, was established and distributed based on IEC 61508. ISO 26262 presents safety analysis method throughout the life cycle from concept stage to operation and disposal. Typical safety analysis methods include PHA (Preliminary Hazard Analysis), HAZOP (Hazard and Operability), FMEA (Failure Mode and Effect Analysis), and FTA (Fault Tree Analysis). However, this analysis method has limitations in analyzing the interactions between modern complex systems. To overcome this, a STPA (System Theoretic Process Analysis) technique based on MIT's STAMP (System Theoretic Accidents Model) model has been proposed. In this paper, as a safety analysis method using STPA, a usecase that defines the system operation process and a risk identification method using STPA are presented. Applying this method to the system development process can contribute to deriving potential risks, causes of risks, and safety requirements, and is expected to improve the quality of the system and reduce costs. For the verification of this study, the ACC (Adaptive Cruise Control) case among the ADAS (Advanced Driver Assistance System) functions of the vehicle is applied and presented.

Keywords: STPA; STAMP; ISO 26262; Autonomous Vehicle; Safety; Safety Analysis; Hazard identification

H. Wu et al. (Eds.): CSIEDE 2022, ACSR 103, pp. 144–153, 2022.
https://doi.org/10.2991/978-94-6463-108-1_17

1 Introduction

Recently, the use of electric and electronic control systems is increasing in various industrial fields such as medicine, nuclear power, aerospace, railway, and automobiles. The increase in electrical and electronic control systems has greatly increased the complexity of designing the system. Due to such a complex system, safety accidents due to malfunctions appeared as a new issue. In particular, in the automobile industry, as the demand and supply for advanced functions such as ADAS (Advanced Driver Assistance System) expand, the existing machine-oriented automobiles have changed to electric and electronic control systems. However, as the use of electric and electronic control systems increased, the complexity of in-vehicle designs increased rapidly, which caused malfunctions throughout the system. Although the IEC 61508 standard, which is a functional safety standard for electrical/electronic/programmable electronic safety management systems across industries, exists, there is a limit to reflect the specificity of automobiles [1]. Therefore, the ISO 26262 functional safety standard specialized for automobiles was established and distributed based on IEC 61508 [2]. ISO 26262 proposes the use of safety analysis techniques such as PHA (Preliminary Hazard Analysis), HAZOP (Hazard and Operability), FMEA (Failure Mode and Effect Analysis), and FTA (Failure Tree Analysis) to identify system malfunctions and risks throughout the life cycle from concept stage to operation and disposal. This analysis method includes the theory that the chain of event model causes accidents due to continuous errors between components [3]. However, existing techniques have limitations in identifying risks arising from interactions between modern complex systems [4]. To overcome these limitations, a STPA (System Theoretic Process Analysis) technique based on the STAMP (System Theoretic Accident Model and Processes) model has recently been proposed [5]. STPA has the advantage of being able to identify risks by identifying UCA (Unsafe Control Actions) that occur in interactions between system components.

This paper defines the system operation process using the safety analysis method using STPA and presents a risk identification method applying Usecase and STPA. In addition, verification is performed by applying an ACC (Adaptive Cruise Control) system case among ADAS (Advanced Driver Assistance System) functions of the vehicle.

The composition of this paper is as follows. Chapter 2, which follows, defines related studies and problems, and introduces ISO 26262-based safety analysis procedures using STPA. Chapter 4 performs verification through application to automobile ACC cases, and Chapter 5 concludes with a summary.

2 Related Work and problem definition

2.1 Background Theory

1) ISO 26262 International Standard for Automotive.

Figure 1 shows the composition of ISO 26262 [2]. It presents safety-related requirements in the entire life cycle from development to production and disposal. Both HW and SW follow the V model development process, and after designing the system, it has a structure that enables HW and SW development to run independently.

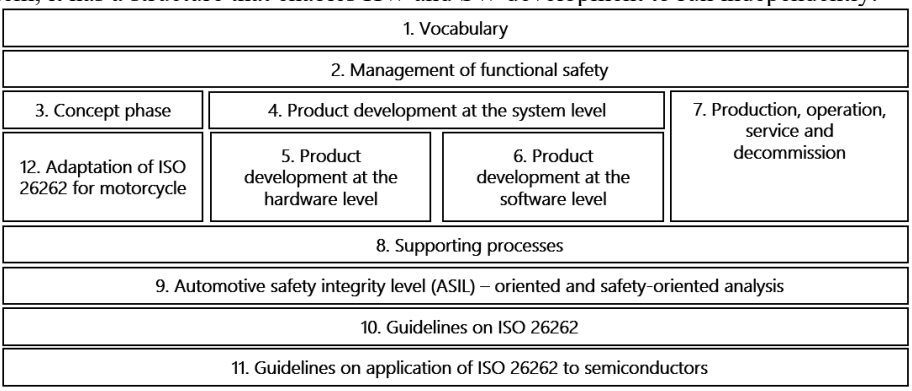

Fig. 1. ISO 26262 Sturecture

2) Safety Analysis.

FTA (Fault Tree Analysis): FTA is a deductive methodology that analyzes in terms of the probability of a defect, specifically defines a failure, and reveals all causes that cause failure using a combination of logic gates. The failure and the cause of the failure are organized in a tree form, and the failure constitutes the highest event of the FTA, and generally represents a very serious failure. The final cause of failure is located at the lowest level, the root of the FTA.

FMEA (Failure Mode and Effect Analysis): FMEA defines how to reduce or avoid the occurrence of failure modes by analyzing their effects on the system. FMEA measures the severity, occurrence, and detection probabilities and calculates the results of the identified failure modes to identify potential failure modes and causes for system components in the initial development process.

HAZOP (Hazard and Operability): HAZOP is a technique that analyzes the risk of a system by deriving a system or all deviation scenarios, and checks whether deviations from design intentions occur and problems caused by them. Analyze possible risks using guide words.

2.2 Related Work

Chen L. et al. (2020) proposed a new method called STPAFT that combines STPA and FMEA with the advantages of both STPA and FMEA. The analysis result of STPAF confirmed that the requirements of ISO26262 can be satisfied [6]. Ishimatsu, T. et al (2010) evaluated the feasibility and usefulness of STPA for the initial system design stage. Using STPA, it is possible to identify the safety requirements and safety constraints of the system before detailed design, and it is also possible to identify risk

scenarios [7]. Hommes (2015) proposed a method to apply STPA to risk analysis using HAZOP in the ISO 26262 concept development stage and safety analysis using FMEA [8]. Thomas (2015) proposed a method of applying STPA in the ISO 26262 development process in developing a vehicle control system. By repeatedly applying STPA, more risks could be identified [9]. Abdulkhaleq, A. et al. (2017) presented the concept of how to use STPA to extend the safety scope of ISO 26262 and support the Hazard Analysis and Risk Assessments (HARA) process. As a result of verification by applying it to Continental's current fully automated vehicle project, it was concluded that STPA is an effective and efficient approach for deriving detailed safety constraints [10].

2.3 Problem Definition

The existing safety analysis technique is a safety analysis technique based on the Chain of Event model, which is suitable for an era when mechanical devices were the mainstay. However, there is a limit to dealing with failures caused by the interaction between elements constituting modern complex systems. A method for risk analysis of complex electrical and electronic systems mounted on today's ISO 26262 vehicles is needed.

3 Safety Analysis Based on ISO 26262 Using STPA

3.1 Objective and Scope of STPA

The risk analysis technique based on STAMP is a technique that analyzes potential risks and causes at the system level throughout the life cycle of the system. STPA does not recognize the problem as a failure of a specific function or a component error, but on the premise that it arises from a control problem between the system and the system or components. STPA-based hazard analysis consists of analyzing the system from a control point of view and identifying inappropriate controls where a hazard may arise. STPA is a top-down analysis method that starts from the definition of an accident and derives a causal scenario. The procedure consists of 4 steps.

3.2 Procedure for performing STPA

1) Accident and Hazard Definition.

STPA This is the stage of determining what kind of accident the purpose of risk analysis is to prevent and determining the scope of the system to be analyzed. The definition of the analysis purpose is further divided into detailed steps such as accident definition, system-level risk definition, and system-level safety constraint derivation.

2) Schematic of Control Structure.

Figure 2 shows the control structure as a control point and composes the loop type composed of subject and object, and control and reaction. As shown in Figure 2, the simplest control structure can show a more complex structure as it goes through the process of refinement.

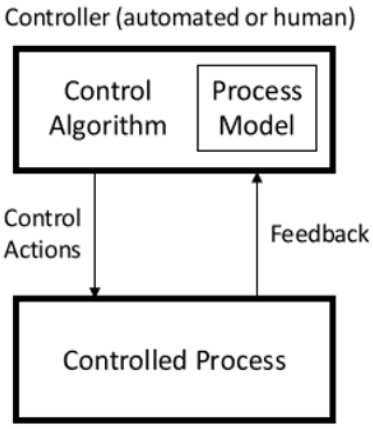

Fig. 2. Common Corms of Control Loop

3) Derivation of UCA (Unsafe Control Action).

UCA means an insecure form of CA (Control Action) that can cause system risk. In order to derive UCA, the form in which the controller provides CA and the situation or conditions under which the CA is performed are largely required. Forms in which CA can be insecure are roughly classified into four types as shown in Table 1. UCA is derived by combining these four types of CA.

Table 1. STPA Guide words

STPA Guide Words	***Unstable Control Command Type***
Not providing	No control command to be performed
Providing Causes	Incorrect or unstable control commands performed
Too Late or Early	Control commands are performed earlier or later
Too Soon or Long	Control commands stop earlier than scheduled, or stay late

4) Derivation of causal scenarios.

Analyze the cause of why the UCA that can cause the risk derived in step 3 occurred. Causes can be classified into two types: why the CA was provided insecurely, and the cause of the CA being improperly performed or not performed. The rim shows two types of cause. Finally, based on these causes, a cause scenario is created.

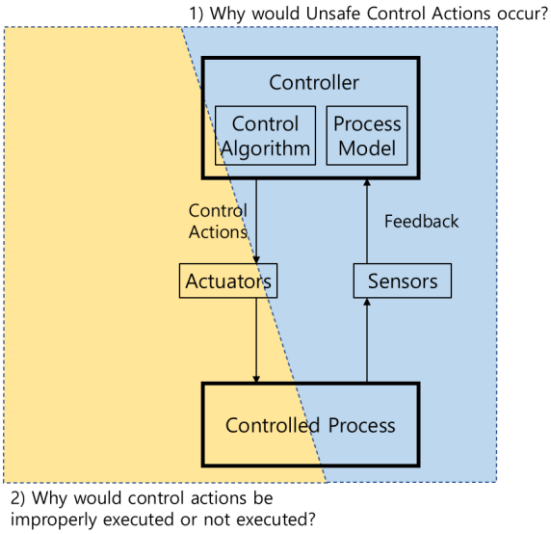

Fig. 3. Identification Causal Scenario

3.3 Integrated ISO 26262 and STPA

Figure 4 shows an example of using ISO 26262 part 3 concept phase and STPA. The control structure diagram of STPA phase 0 shows the main components of the system under analysis and uses a list of hazards, accidents, and high levels of system safety constraints identified in STPA phase 0 as input to the HARA approach of ISO 26262. Hazardous events, safety goals, situations and modes obtained as a result of HARA are used as inputs to STPA phase 1 to identify unsafe control tasks. Identify unstable scenarios and use the results to develop system functional safety concepts and safety requirements at this level.

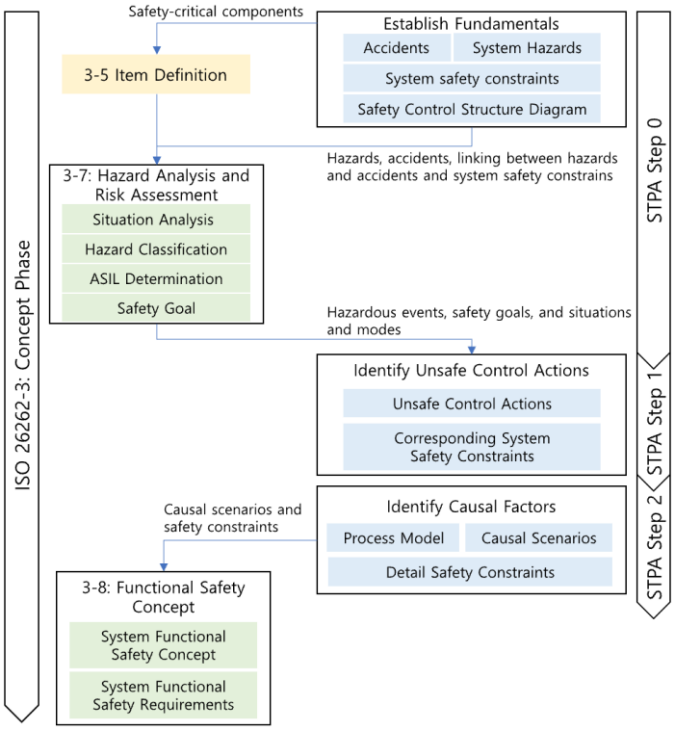

Fig. 4. Integration of STPA and ISO 26262

4 STPA application case stury

ACC is one of the ADAS functions widely applied to today's vehicles, and it is a system that automatically maintains an appropriate distance from the vehicle in front using a radar mounted on the front of the vehicle. The procedure for applying STPA to the ACC system is as follows.

4.1 Accident and Hazard Definition

As shown in Table 2, accidents and hazards can be identified at the system level.

Table 2. Accidents and hazard Identification

Accident	A1	car collision
	A2	Collision with moving obstacles
Hazard	H1	Not keeping a safe distance from other vehicles
	H2	Not keeping a safe distance from other obstacles

4.2 Schematic of Control Structure

ACC consists of driver, ACC module, radar, brake and accelerator. The ACC function can be turned on/off, and the ACC module can command Accelerate and Decelerate. CA of ACC system can be expressed as Accelerate and Decelerate, and Control Structure can be expressed as Figure 5.

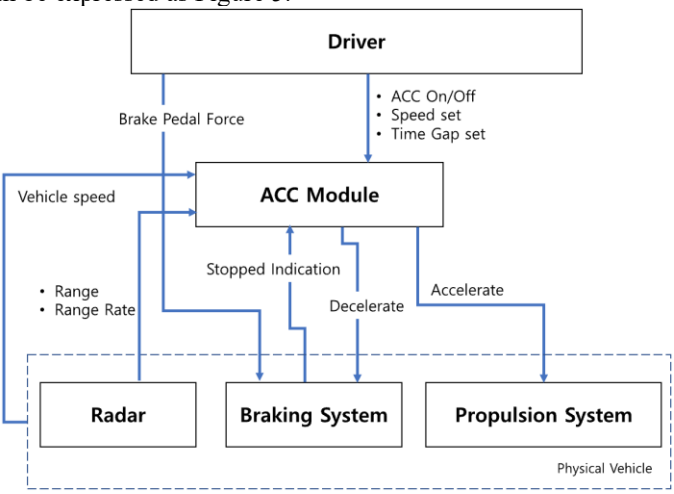

Fig. 5. Adaptive Cruise Constrol System Control Structure

4.3 Derivation of UCA (Unsafe Control Action)

Table 3 shows the results of identifying UCA by applying four patterns to CA of the ACC system.

Table 3. UCA identification

CA	*Not providing*	*Providing Causes*	*Too Late or Early*	*Too Soon or Long*
Accelerate	UCA1: Acceleration does not occur even when there are no vehicles and obstacles in front	UCA2: The set speed has already been reached but accelerated	UCA3: Acceleration is performed before the ACC function is activated.	UCA4: Accelerate beyond the set speed
	-	UCA5: Close to the vehicle in front but accelerate	UCA6: Acceleration is applied late after the ACC function is activated	UCA7: Violation of the safe distance from the vehicle in front due to long acceleration time
Decelerate	UCA8: No deceleration in the presence of vehicles and obstacles ahead	-	UCA9: Decelerate too late after finding an obstacle	-

Based on the UCA derivation result, the safety constraint that the ACC system should have can be expressed as follows.

- ACC cannot exceed the speed limit and distance set by the driver
- ACC should not crash
- ACC must not be activated before the operator activates the function

4.4 Derivation of causal scenarios

The results of deriving the causal scenario for 'UCA5 (close to the vehicle in front but accelerated)' among the identified UCAs are as follows.

- Algorithm does not accurately calculate distance to vehicle in front
- Inability to function normally due to deterioration of brake performance
- Brake not providing the required force to decelerate

4.5 Comparison of FMEA and STPA

Table 4 shows the comparison between FMEA and STPA. FMEA has limitations in analyzing complex systems today as shown in Table 4, as shown in Figure 5, because risk analysis is possible only on a single system. Therefore, it is more useful to apply STPA than FMEA in such complex systems.

Table 4. Comparison of FMEA and STPA

System	***STPA***	***FMEA***
Single systme	Can be performed	Can be performed
Interworking system	Can be performed	Inability to performance
Complex system	Can be performed	Inability to performance

5 Conclusion

In the past, safety analysis techniques such as FTA, FMEA, and HAZOP were used by focusing on the cause of accidents on the failure of components constituting the system. However, it was found that the cause of the accident was not only by a single component, but also by an interaction between systems or between systems and components. To overcome this problem, MIT presented a new STPA safety analysis technique based on the STAMP model. In this paper, we looked at how STPA can be used in the existing ISO 26262 automotive functional safety. Also, the process of deriving risk cause scenarios by applying STPA to the ACC function, which is one of the ADAS functions, was examined. If this study is applied to the system development process, it can contribute to deriving many potential risks, causes, and safety require-

ments in the system. In addition, it is expected that this will improve system quality and reduce costs. In this study, only ACC was applied, but in the future, it will be applied to various functions and systems used in automobiles.

Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression, “One of us (R. B. G.) thanks . . .” Instead, try “R. B. G. thanks”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

References

1. “IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems,” IEC, 2010.
2. “ISO 26262 : Road Vehicles –Functional Safety,” ISO, 2018.
3. L. Benner, “Accident investigations: Multilinear events sequencing methods,” Journal of safety research, 7(2), pp. 67-73, 1975.
4. N. Leveson, “A New Accident Model for Engineering Safer systems,” Safety science, 42(4), pp. 237-270, 2004.
5. N. G. Leveson, “Engineering a safer world: Systems thinking applied to safety,” The MIT Press. pp. 560, 2016
6. L. Chen, J. Jiao, and T. Zhao, “A Novel Hazard Analysis and Risk Assessment Approach for Road Vehicle Functional Safety through Integrating STPA with FMEA,” Applied Sciences, vol. 10(21), 7400, pp. 1-23, 2020.
7. T. Ishimatsu, N. G. Leveson, J. Thomas, M. Katahira, Y. Miyamoto, and H. Nakao, “Modeling and Hazard Analysis Using Stpa,” Proceedings of the 4th IAASS Conference, Making Safety Matter, 19–21 May 2010, Huntsville, Alabama, USA SP-680, pp. 1-10, 2010.
8. V. E. Hommes, “Safety Analysis Approaches for Automotive Electronic Control Systems,” Society of Automotive Engineers’ Meeting, pp. 1-16 2015.
9. J. P. Thomas, “Iterative Application of STPA for an Automotive System,” STAMP Workshop Presentation, pp. 1-27, 2015.
10. A. Abdulkhaleq, S. Wagner, D. Lammering, H. Boehmert, and P. Blueher, “Using STPA in compliance with ISO 26262 for developing a safe architecture for fully automated vehicles,” arXiv preprint arXiv:1703.03657, pp. 1-14, 2017