ISSN: 2633-4828 Vol. 5, No.3, September, 2023

International Journal of Applied Engineering and Technology

Comparison and Combination of Hazard and Operability Analysis and System Theoretic Process Analysis Applied to Functional Safety—A Case Study of Traffic Jam Pilot System

Lei He[1]
[1]Associate Professor, College of Automotive Engineering, Jilin University, Changchun, China.
jlu_helei@jlu.edu.cn

Feng Ye[2], Xiucai Zhang[3]
[2,3]MS Scholar, Automotive engineering with the State Key Laboratory of Automotive Simulation and Control, Jilin University, Changchun, China.
yefeng21@mails.jlu.edu.cn[2], zhangxc21@mails.jlu.edu.cn[3]

Zhongju Di[4]
[4]China FAW Group Corporation, China
dizhongju@faw.com.cn

Date of Submission: 09th July 2023 Revised: 23th August 2023 Accepted: 29th August 2023

How to Cite: Lei He, Feng Ye, Xiucai Zhang and Zhongju Di. (2023). Comparison and Combination of Hazard and Operability Analysis and System Theoretic Process Analysis Applied to Functional Safety——A Case Study of Traffic Jam Pilot System. International Journal of Applied Engineering and Technology 5(3), pp. 41-50.

***Abstract* - With the continuous development of autonomous driving and vehicle electrification, vehicle functions have become increasingly comprehensive, while the electronic and electrical systems inside vehicles have become increasingly complex. The interaction between systems has become increasingly frequent and ensuring the safety of autonomous vehicles has become a major concern. Functional safety is designed to address safety issues caused by failures in the electronic and electrical systems of vehicles. Hazard analysis is a critical step in the functional safety development process. In this study, Hazard and Operability Analysis (HAZOP) and System Theoretic Process Analysis (STPA) are respectively used to carry out functional safety vehicle hazard analysis with an open automatic driving system Traffic Jam Pilot (TJP) as an example, and the analysis results are com-pared. The comparison shows that the two methods can obtain the same vehicle hazard results in the functional safety analysis of automatic driving system, but each has its advantages and limitations in the process. Based on the strengths and weaknesses of both methods, a idea approach that combines the two methods is proposed.**

***Index Terms* - Functional Safety, HAZOP, ISO 26262, STPA**

INTRODUCTION

Safety has always been a key focus of the autonomous driving industry, and the safety of the technology determines the likelihood of its market acceptance and consumer recognition. To address safety issues in the automotive industry, vehicle safety is divided into functional safety, Safety of the Intended Functionality, and Cybersecurity engineering. In 2011, the International Organization for Standardization proposed ISO 26262 - Functional Safety, which is defined as "ISO 26262 aims to address safety issues caused by failures in electronic and electrical systems and their interactions," and it is the standard set to address vehicle functional safety issues [1].

Functional safety emphasizes system failures that need to be addressed and provides a standard for the design and development cycle of vehicle systems.

In the functional safety V-model development process, it is necessary to first de-fine the items for the pre-development system, including the system's functions, operating design domain, actuator capabilities or capability assumptions, and initial system architecture. After completing the initial definition of these items, it is necessary to perform risk and hazard analysis on the system. ISO 26262 functional safety standard recommends several hazard analysis methods, including Fault Tree Analysis (FTA), Failure Modes and Effects Analysis (FMEA), and Hazard and Operability Analysis (HAZOP). Through the results of the completed hazard analysis, safety goals can be derived, and safety requirements can then be deduced.

Regarding the hazard analysis methods recommended by ISO 26262, they are all based on reliability theory. However, these recommended methods may not be suitable for existing autonomous driving systems due to their complexity and diversity of interactions among components. In particular, with the advent of the era of autonomous driving, the exchange of information between the autonomous driving system and the external environment has become a critical component. Traditional hazard analysis methods such as FTA and FMEA are not suitable for such open systems, and are no longer capable of meeting the needs of hazard analysis for autonomous driving functional safety.

HAZARD ANALYSIS METHODOLOGY

I. Fault Tree Analysis

Fault Tree Analysis (FTA) is a top-down deductive failure analysis method that can be used for both quantitative and qualitative analysis [2]. This method was first proposed by Waston in 1961 when researching the safety of the Minuteman missile launch control system [3]. Fault trees are based on fault relationships and have clear causal relationships, which helps to understand the various causes and logical relationships that lead to accidents. However, FTA has certain limitations when analyzing process or equipment systems, and the analysis results may vary depending on the analyst's experience and familiarity with different objects being analyzed. For overly complex systems, the FTA may become too large, making calculations more difficult. The authors in [4] applied FTA to safety-oriented system hardware architecture, satisfying the safety requirements of ISO 26262 and efficiently addressing hardware cost constraints. The study in [5] compared FTA with System Theoretic Process Analysis (STPA) methods used in Brake-by-Wire systems and found that FTA analysis results lack generality compared to STPA.

II. Failure Mode and Effects Analysis

Failure Mode and Effects Analysis (FMEA) is a bottom-up inductive analysis method that allows for easy and cost-effective modifications to products or processes, reducing the cost of modifications after harm has occurred. This method can identify measures to avoid or reduce potential failures. Similar to FTA, FMEA is based on the failure chain accident model and the preventive mechanisms derived from the analysis are often achieved by enhancing component reliability or redundancy. The authors in [6] introduced an improved FMEA method based on fuzzy rule base and gray relation degree into functional safety analysis. The concept of Failure Mode and Effects Analysis for Monitoring and System Response (FMEA-MSR) was proposed in [7] as a supplementary method for monitoring system response and analyzed potential failure causes under customer operating conditions.

III. Hazard and Operability Analysis

Hazard and Operability Analysis (HAZOP) is an exploratory method based on functional hierarchy that presets the possible faults and hazards of existing functions through predetermined guide words, and analyzes the consequences caused by these faults and hazards. However, HAZOP has certain limitations. It often relies on the experience of the participants in the analysis, and when complex systems fail, the impact is often not caused by a single factor. Therefore, using HAZOP may result in incomplete analysis.

The authors in [8] studied the applications of STPA, HAZOP, and Pre-liminary Hazard Analysis (PHA) in risk analysis of autonomous marine systems, and found that HAZOP performed better than the other two methods in analyzing environmental impacts and human-machine interactions. The authors in [9] improved the HAZOP guide words by combining them with the execution style of software, and developed a more detailed set of guide words.

IV. System Theoretic Process Analysis

System Theoretic Process Analysis (STPA) was proposed by Professor NANCY G. LEVESON from Massachusetts Institute of Technology around 2000. After being verified and discussed by many scholars, this method has been widely applied in the fields of industrial safety, food safety, and aviation accident analysis, and has achieved good results. The study in [10] applied STPA to the ISO 26262 standard process and provided an excerpt on how to apply STPA to automotive subsystems based on the ISO 26262 concept phase. The authors in [11] conducted a study on the expected functional safety of the Lane Keeping Assistance (LKA) system based on STPA, established an LKA system control model, identified unsafe control behaviors using the STPA method, and proposed vehicle-level safety constraints.

STPA is a hazard analysis technique based on an accident causation and propagation model. Compared to other traditional functional safety hazard analysis methods, STPA is better at analyzing complex systems, identifying safety requirements and constraints in the early conceptual analysis phase, and improving the safety of system de-sign by changing the system architecture in the system design phase. By identifying safety requirements and constraints in the conceptual analysis phase of functional safety, STPA can eliminate the cost of redesign caused by defects in the later stages of development.

The basic steps of STPA are as follows:

- Define the analysis objective: clarify the loss, hazard, system description, and system boundary to be analyzed, and determine the safety constraints at the system level.
- Establish a control structure.
- Identify unsafe control actions: Unsafe Control Actions (UCAs) refer to control actions that may cause hazards in specific situations and worst-case scenarios, and can be simplified into four categories: Required but not provided, Provided but not required, Provided but wrong timing, and Provided but incorrect duration.
- Identify scenarios that lead to losses.

As can be seen, the hazard analysis methods recommended by ISO 26262 exhibit limitations when dealing with complex systems, especially with the increasing complexity of system components and closer system interactions in the era of autonomous driving.

The ISO 26262 recommended methods are no longer sufficient to meet the functional safety requirements of autonomous driving.

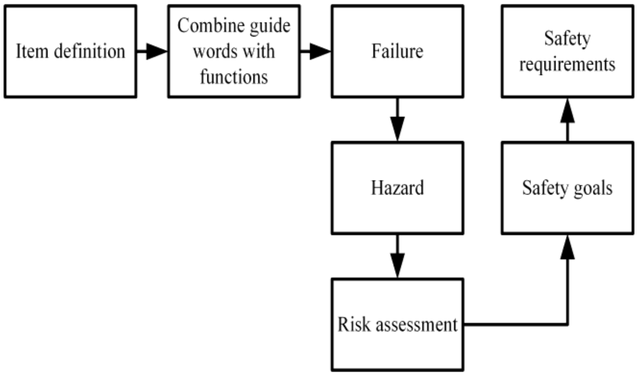

FIGURE 1 APPLICATION OF HAZOP TO ISO 26262

STPA, as a new hazard analysis method, is better at analyzing complex systems compared to other three methods.

Therefore, it has gradually been applied in the field of vehicle safety analysis as vehicles enter the era of autonomous driving. This paper will apply the STPA and HAZOP analysis methods to study the safety of autonomous driving systems, in order to com-pare the differences between the two methods.

V. Application of HAZOP to ISO 26262

The application of HAZOP in the field of functional safety has become relatively mature. The key to its application lies in the completeness of the definition of the system's functions, which relies heavily on the expertise of experts. The selection of ap-propriate guide words also affects the analysis results and workload. Since the standard does not specify the selection of guide words for autonomous driving systems, guide words need to be selected according to the needs. The selection of guide words should ensure the coverage of system hazard analysis and reduce analysis redundancy to minimize workload. The analysis process of HAZOP in the field of functional safety is shown in Figure 1.

VI. Application of STPA to ISO 26262

With the advancement of autonomous driving technology, system components have become increasingly complex and interactions between components have become more frequent. To address the issue of functional safety risk analysis for autonomous vehicles, STPA has been introduced. In the STPA analysis process, the analysis of system functional safety hazards is not mandatory. When applying STPA to functional safety risk analysis, certain adjustments need to be made, and the final step-by-step principle diagram is shown in Figure 2.

VEHICLE HAZARD ANALYSIS

I. TJP System Introduction

Traffic Jam Pilot (TJP) is a system with certain autonomous driving functions de-signed to cope with urban traffic-congestion in low-speed conditions (below 60km/h). Its specific functions include automatic following, automatic braking, automatic lane changing, and lane keeping.

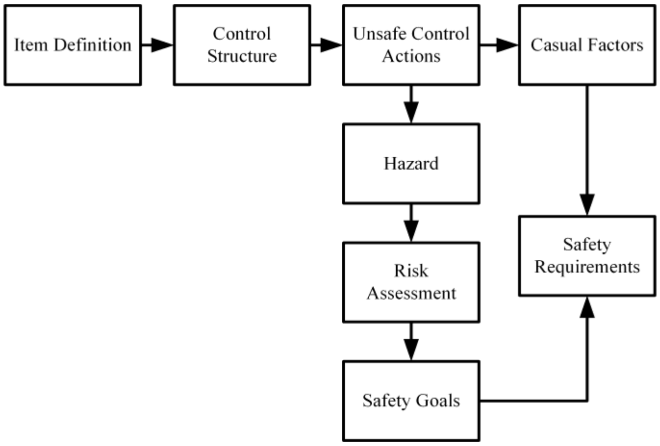

FIGURE 2 APPLICATION OF STPA TO ISO 26262

II. Operational Design Domain Definition

The TJP system analyzed in this paper is designed for driving on urban traffic congested roads at low speeds (0-60km/h). To ensure the proper functioning of the system, clear lane markings (or median barriers for oncoming traffic) are needed, and traffic participants include adjacent lane vehicles traveling in the same direction and oncoming traffic, as well as pedestrians and non-motorized vehicles that may lack rule constraints. Temporary traffic events should be set as events that will not affect the normal functioning of the system and at least one lane should be kept clear, and environmental conditions should not affect the system's functions (such as flooded urban road surfaces). To achieve high-level autonomous driving conditions and functions, high-precision maps are set at the information layer.

III. Basic Architecture of TJP System

TJP is a type of L3 autonomous driving system that requires ensuring the integrity of the perception system's interaction with the external environment and the accuracy of decision-making and path planning during dynamic driving tasks. A complete L3 autonomous driving system should be capable of independently and safely completing dynamic driving tasks. Radars and cameras act as collection sensors for external environmental data, providing real-time monitoring of obstacles in the external environment, whereas high-precision maps typically serve as auxiliary tools for executing dynamic driving tasks.

Although L3 autonomous driving systems are not considered high-level autonomous driving, they still require considering the interaction between the driver and the vehicle. In the TJP system, the human-machine interaction system assumes this task.

At the same time, the ECU calculator requires the vehicle's own state parameters and environmental perception data to perform decision-making and planning, while the vehicle state sensor is used to monitor the vehicle's own state.

TABLE I
HAZOP ANALYSIS OF HMI MODULE

ID	Functions	Guide Words	Failure	Hazard
01	TJP system switch	Loss	The driver cannot actively switch the TJP function.	H1
02		Stuck	When the driver starts or close, the TJP system still maintains the original state.	H1
03		Late	When the driver starts or closed, TJP will not respond after a period of delay for a period of time.	H1
04	Warning system	Loss	TJP system is unable to provide driver alerts during operation.	H2
05		Wrong	During the operation of the TJP system, the driver receives an incorrect warning.	H3
06		Late	During the operation of the TJP system, the driver's warning reminded too late.	H4
07	Driver monitoring system	Loss	During the operation of the TJP system, the driver monitoring system is unable to monitor the driver's state.	H2
08		Wrong	During the operation of the TJP system, the driver monitoring system incorrectly identifies the driver's state.	H3
09		Late	During the operation of the TJP system, the driver monitoring system identifies the driver's state too late.	H4

TABLE II
HAZOP ANALYSIS OF PERCEPTION FUNCTION MODULE

ID	Functions	Guide Words	Failure	Hazard
10	Image data processing	Loss	Cannot process image data.	H5 H6
11		More	Key image frames are missing, resulting in too few recognized targets or no targets being recognized.	H5 H6
12		Less	There is too much noise, causing ghosting or ghost images to appear.	H7 H8
13		Wrong	There was an error in image processing, resulting in incorrect recognition.	H7 H8
14		Stuck	Image data processing was completed, but the processing results were not submitted in a timely manner.	H5 H6
15	Point cloud data processing	Loss	False targets were not removed, affecting the perception system results.	H7 H8
16		More	Too few targets were recognized.	H5 H6
17		Less	Too many targets were detected, causing excessive computational load.	H7 H8
18		Wrong	Incorrect processing of the point cloud signal resulted in failure.	H5 H6
19	Object detection	Loss	During the operation of the TJP system, the system cannot recognize obstacle targets.	H5 H6
20		Less	During the operation of the TJP system, the system cannot recognize obstacle targets.	H5 H6
21		Wrong	During the operation of the TJP system, the system incorrectly recognizes obstacle targets.	H7 H8
22		Late	During the operation of the TJP system, the system identifies obstacle	H12 H13

			targets too late.	
23	Sensor fusion	Loss	Unable to process data transmitted by sensors.	H5 H6
24		Less	Insufficient data processing capabilities, unable to recognize obstacles or risks.	H5 H6
25		More	Processing too much data results in excessive computational load.	H12 H13
26		Wrong	Incorrect processing of data leads to failure to detect obstacles or risks.	H5 H6
27		Late	Data processing is too late, and the system cannot respond to risks in time.	H12 H13

The computed control behavior will be used to control the vehicle through the entire vehicle control system. Due to the comprehensive functions of the TJP system, the subsystems in the entire vehicle control system should include the braking system, steering system, and drive system.

IV. Execution of HAZOP

In the context of ISO 26262 functional safety analysis at the vehicle level, this paper employs HAZOP to analyze the hazards associated with the TJP system from a functional perspective.

The TJP system is divided into four functional modules: human-machine interaction, perception, decision-making and planning, and control. The expected functions of the TJP system are defined based on these modules, and appropriate guide words are selected to identify failure scenarios and derive vehicle-level hazards. The definition of expected functions and the selection of guide words determine the workload and coverage of the HAZOP analysis. The more complex the functional definition, the greater the workload, and the more comprehensive the definition of guide words, the broader the coverage of potential hazards.

TABLE III
HAZOP ANALYSIS OF PLANNING/DECISION MODULE

ID	Functions	Guide Words	Failure	Hazard
28	Path planning	Loss	Path planning cannot be carried out when obstacles are present.	H5
29		Wrong	Planned the wrong route.	H13
30		Late	The execution of the path planning function was delayed.	H13
31	Car-Following	Loss	The vehicle cannot automatically follow the front vehicle.	H9
32	Vehicle following distance maintenance	Loss	The vehicle cannot maintain a safe following distance from the front vehicle.	H10
33		More	The distance between the vehicle and the preceding vehicle is too far.	H9
34		Less	The vehicle cannot maintain a safe following distance from the front vehicle.	H10
35		Wrong	The vehicle cannot maintain a safe following distance from the front vehicle.	H10
36	Scenes understanding	Loss	The system cannot understand the scene.	H5 H6
37		Wrong	The system has incorrect scene understanding.	H5 H6
38		Late	Delayed scene understanding leads to system response lag.	H12 H13

TABLE IV
HAZOP ANALYSIS OF CONTROL MODULE

ID	Functions	Guide Words	Failure	Hazard
39	Acceleration function	Loss	During the operation of the TJP system, the vehicle loses its acceleration function.	H9
40		More	During the operation of the TJP system, the vehicle is provided with too much acceleration.	H10
41		Less	During the operation of the TJP system, the vehicle is provided with too little acceleration.	H9
42		Wrong	During the operation of the TJP system, acceleration is provided to the vehicle when it is not needed.	H10
43		Stuck	During the operation of the TJP system, the vehicle experiences acceleration lag.	H9
44		Late	During the operation of the TJP system, the vehicle is provided with acceleration too late.	H9
45	Braking function	Loss	During the operation of the TJP system, the vehicle is unable to brake.	H6
46		More	During the operation of the TJP system, the vehicle brakes frequently.	H11
47		Less	During the operation of the TJP system, the vehicle is not provided with enough braking force.	H12
48		Wrong	During the operation of the TJP system, braking force is provided to the vehicle when it is not needed.	H8
49		Stuck	During the operation of the TJP system, the vehicle experiences braking lag.	H6
50		Late	During the operation of the TJP system, the vehicle is provided with braking force too late.	H12

51	Steering function	Loss	During the operation of the TJP system, the vehicle cannot be provided with steering torque.	H5
52		More	During the operation of the TJP system, the vehicle is provided with too much steering torque.	H13
53		Less	During the operation of the TJP system, the vehicle is not provided with enough steering torque.	H13
54		Wrong	During the operation of the TJP system, the vehicle is provided with incorrect steering torque.	H7
55		Stuck	During the operation of the TJP system, the vehicle experiences steering torque lag.	H13
56		Late	During the operation of the TJP system, the vehicle is provided with steering torque too late.	H13

Different regulatory standards have different definitions of guide words for HAZOP. Currently, two main standards are widely used: IEC 61882 and SAE J2980. After comprehensive analysis and selection, the guide words selected for the TJP system are Loss, More, Less, Wrong, Stuck, Early, and Late. Using HAZOP for safety analysis of the TJP system, the results are shown in Table I, Table II, Table III, and Table IV.

V. Execution of STPA

After defining the relevant items, the control structure is further developed based on the expected functions as shown in Figure 3. The control unit of the TJP system is divided into the driver, external environment, human-machine interaction module, sensors, perception module, decision-making module, basic vehicle systems, and vehicle chassis. The dashed line represents the interaction between internal components of the system, whereas the components outside the dashed line represent external com-ponents that interact with the system.

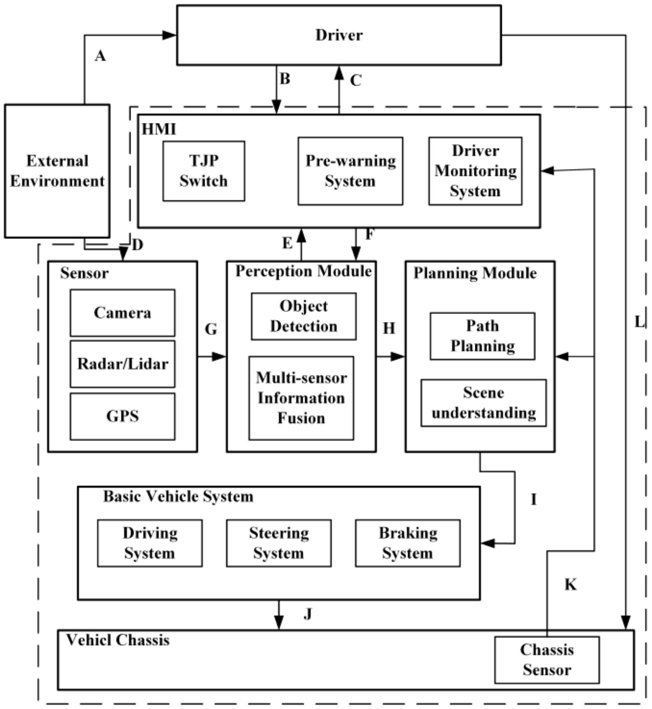

FIGURE 3 TJP SYSTEM CONTROL STRUCTURE

Control actions of control structures:

A. The driver directly observes the external environment through visual perception.
B. The driver turns on/off the TJP system.
C. The human-machine interaction system provides warnings to the driver and monitors the driver's state.
D. External environmental information is collected by sensors.
E. System status.
F. The interactive switch turns on/off the TJP system.
G. Sensor information is transmitted to the perception module for data processing.
H. Processed perception data is used for path planning by the decision module.
I. Adjustments are made to the vehicle's basic systems, including the power system, steering system, and braking system.
J. The basic vehicle system adjusts throttle opening, steering torque, and braking torque.
K. Chassis sensors transmit vehicle state parameters to the decision module and human-machine interaction module.
L. The driver directly operates the vehicle.

Combining the control action of control structures with four predefined scenarios, we analyze unsafe control action. Unsafe control action of the system can result in vehicle-level hazard. The specific analysis results are summarized in Table V.

TABLE V
STPA ANALYSES HAZARDS FOR TJP CONTROL STRUCTURES

ID	Key Control Actions	Predefined scenarios	Unsafe Control Actions	Hazard
01	The human-machine interaction system provides warnings to the driver.	Provided but not required	Providing warnings when driver warnings are not needed.	H3
02		Required but not provided	Providing no warnings when driver warnings are needed.	H2
03		Provided but wrong timing	Providing warnings to the driver but too late.	H4
04		Provided but incorrect duration (Short duration)	Providing warnings to the driver for too short a time, leading to the driver ignoring the takeover signal.	H2
05	Human-machine interaction system monitors driver status.	Required but not provided	Not monitoring the driver's driving status when it is necessary to do so.	H2
06		Provided but wrong timing	Monitoring the driver's status too late.	H4
07	Sensors collect external environmental data.	Required but not provided	Sensors collect external environmental data without providing it.	H5 H6
08		Provided but wrong timing	Collecting information at the wrong time points interferes with the system's operation.	H7 H8
09	Confirming the system's status.	Required but not provided	Not providing the system status when it is necessary to do so.	H2
10		Provided but not required	Providing incorrect system status when it is not necessary to do so.	H3
11		Provided but wrong timing	Providing the system status too late.	H4
12	Interactive switch to turn on/off TJP system.	Provided but not required	TJP system functions are still provided even if the driver turns it off.	H1
13		Required but not provided	The TJP system does not activate even when the driver turns it on.	N/A
14	Sensor data is transmitted to the perception module for data processing.	Provided but not required	Providing incorrect sensor data when it is not necessary to provide sensor data.	H7 H8
15		Required but not provided	Not providing sensor data when it is necessary to do so.	H5 H6
16		Provided but wrong timing	Providing sensor data too late.	H12 H13
17	The decision module obtains processed perception data.	Provided but not required	Providing incorrect perception data when it is not necessary to provide perception data.	H7 H8
18		Required but not provided	Not providing perception data when it is necessary to do so.	H5 H6
19		Provided but wrong timing	Providing perception data too late.	H12 H13
20	Controlling vehicle acceleration.	Provided but not required	Providing vehicle acceleration when it is not necessary to do so.	H10
21		Required but not provided	Not providing vehicle acceleration when it is necessary to do so.	H9
22		Provided but wrong timing	Providing the correct vehicle acceleration but too early.	H10
23		Provided but incorrect duration (Long duration)	Providing the correct vehicle acceleration but for too long of a duration.	H10
24		Provided but incorrect duration (Short duration)	Providing the correct vehicle acceleration but for too short of a duration.	H9
25	Control the steering of the vehicle.	Provided but not required	Providing torque to the vehicle's steering system unnecessarily.	H7
26		Required but not provided	Not providing enough torque to the vehicle's steering system when it is needed.	H5
27		Provided but wrong timing	Not providing enough torque to the vehicle's steering system when it is needed.	H13
28		Provided but incorrect duration (Long duration)	Providing the correct steering torque but for too long of a duration.	H13

29		Provided but incorrect duration (Short duration)	Providing the correct steering torque but for too short of a duration.	H13
30	Control the braking of the vehicle.	Provided but not required	Providing braking force to slow down the vehicle unnecessarily.	H8
31		Required but not provided	Not providing braking force to slow down the vehicle when it is needed.	H6
32		Provided but wrong timing	Providing the correct braking force but too early.	H11
33		Provided but wrong timing	Providing the correct braking force but too late.	H12
34		Provided but incorrect duration (Short duration)	Providing the correct braking force but for too short of a duration.	H12
35	Human-machine interface module obtains vehicle state parameters.	Provided but not required	Providing incorrect vehicle state parameters to the human-machine interface module without the need to do so.	H3
36		Required but not provided	Not providing the necessary vehicle parameters to the human-machine interface module when they are needed.	H2
37		Provided but wrong timing	Providing the correct vehicle state parameters to the human-machine interface module but too late.	H4
38	Decision-making module obtains vehicle state parameters.	Provided but not required	Providing incorrect vehicle state parameters to the decision-making module without the need to do so.	H3
39		Required but not provided	Not providing the necessary vehicle parameters to the decision-making module when they are needed.	H2
40		Provided but wrong timing	Providing the correct vehicle state parameters to the decision-making module but too late.	H4

RESULTS ANALYSIS

Based on the analysis in the previous sections, we conducted HAZOP analysis from a functional perspective and STPA analysis from a control perspective. Using HAZOP analysis, we obtained 56 failure modes and 13 vehicle-level dangers based on predefined expected functions and defined guide words.

Using STPA analysis of the control structure module, we identified 40 unsafe control actions and 13 vehicle-level hazards. Both approaches led to the same vehicle-level hazards, and collate the number of vehicle hazards analyzed by HAZOP and STPA. The specific results are summarized in Table VI.

TABLE VI
HAZOP&STPA ANALYSIS OF TJP SYSTEM RESULTS IN HAZARDS

ID	Hazard Descriptions	HAZOP	STPA
H1	Non -TJP running section, TJP is still running.	3	1
H2	When conditions exist that are beyond the operating capabilities of the TJP system, the driver does not take over.	2	5
H3	If there are no conditions beyond the operating capabilities of the TJP system, the driver warning system alerts the driver with a warning reminder.	2	4
H4	If there are conditions beyond the operating capabilities of the TJP system and the driver takes over too late, it may result in a collision.	2	5
H5	The vehicle did not make an avoidance response when an obstacle was detected.	14	4
H6	The vehicle did not apply the brakes when an obstacle was detected.	14	4
H7	The vehicle made an avoidance response when no obstacle was present.	6	4
H8	The vehicle applied the brakes when no obstacle was present.	6	4
H9	The vehicle still loses track of the target vehicle even though there is a front target vehicle.	6	2
H10	Collision occurs with the target vehicle ahead.	5	3
H11	The vehicle brakes frequently when obstacles or targets appear.	1	1
H12	The vehicle applies the brakes in response to an obstacle, but still collides.	6	4
H13	The vehicle makes an avoidance response to an obstacle, but still collides.	10	5
Total		77	47

According to the hazards caused by system and external interactions (H1 to H4) designated as W, and the hazards caused by internal interaction failures (H5 to H13) designated as N, the analysis results of HAZOP amounted to 9 in the W region, where-as STPA yielded a total of 16 analysis results. When analyzing the vehicle hazards resulting from external interactions, STPA required 78.7% more workload compared to HAZOP. Similarly, in the N region, HAZOP yielded a total of 68 analysis results, whereas STPA produced 31 analysis results. When analyzing the vehicle hazards caused by external interactions, HAZOP required 119.3% more workload compared to STPA. Since a total of thirteen vehicle hazards were ultimately identified, it can be inferred that the greater the number of analysis results, the higher the redundancy in the analysis.

DISCUSSION

Based on the derived hazard analysis results, the HAZOP and STPA methods pro-vide similar results in analyzing vehicle-level dangers in vehicle systems. However, in practical application, HAZOP heavily relies on the analyst's experience, which leads to a high workload and long analysis time. Furthermore, as the complexity of the system increases, the workload also increases. In contrast, the STPA method focuses more on the design of the control structure, and a reasonable control structure can more efficiently facilitate subsequent analysis, thereby shortening the analysis time. The specific differences between the two methods are listed in Table VII.

Based on the results of the comparative analysis, a fusion model that integrates HAZOP and STPA methods can be used for functional safety analysis while retaining their respective advantages and minimizing their drawbacks. The fusion model, as shown in Figure 4, further refines the control modules divided by STPA and assigns the vehicle system functions to the control modules, which are classified into two categories: internal interaction and external interaction. The detailed line box represents the internal interaction analysis module, whereas the bold dotted line box represents the external interaction analysis module. STPA analyzes the interaction of internal control modules, whereas HAZOP analyzes the safety issues of external interaction control modules.

TABLE VII
COMPARISON OF HAZOP AND STPA FOR FUNCTIONAL SAFETY ANALYSIS

Item	HAZOP	STPA
Analysis Aspect	System Function	Control Action
Key Points	Choose right guide words.	Design reasonable control structure.
Applicable System	Open System	Open System
Time Cost	This approach is more time-consuming and the workload increases with the complexity of the functionality.	This method takes less time.
Advantage	Based on the system function, this approach is easier to intuitively understand the damage caused by the function failure of the vehicle, and is better at analyzing the external interaction function failure.	Based on the control action, the interaction between each component will be analyzed, which is easier to cover the fault situation, and is better at analyzing the internal system interaction fault.
Disadvantage	Over-reliance on analyst experience; High cost of time-consuming and labor-intensive analysis;	In the face of open systems, the interaction and control behavior with the outside world is not easy to determine.

The fusion model not only improves the efficiency of the safety analysis process but also enhances the coverage of the safety analysis results. The fusion of safety analysis methods addresses the issues of redundancy and time-consuming processes when applying a single analysis method in safety analysis. The fusion of safety analysis methods is expected to be increasingly applied in the academic and engineering domains of safety analysis in the future.

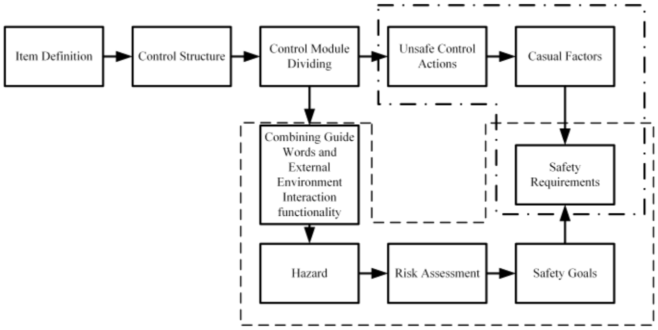

FIGURE 4 FUNCTIONAL SAFETY ANALYSIS METHOD OF HAZOP&STPA FUSION

CONCLUSION

Both HAZOP and STPA methods can be used in the hazard analysis of open systems in autonomous driving vehicles. The analysis results from both methods are generally similar. HAZOP method identifies deviations using system parameters and guide words, but it is a time-consuming task that heavily relies on the knowledge and expertise of experts.

On the other hand, STPA method predefines four classes of unsafe control actions to identify hazards, but when it comes to external interactive systems, the control actions of operators cannot simply be categorized into the four predefined control actions, resulting in poorer analysis results. The fusion of HAZOP and STPA methods for functional safety analysis is a future research direction.

ACKNOWLEDGMENT

This research was supported by the project on research and development of intelligent vehicle key technologies and industrialization projects based on new energy vehicles under Grant TC210H02S and by the project on quantitative development and measurement technology research of expected functional safety based on vehicle-cloud collaboration under Grant 20220301012GX.

COPYRIGHT FORM

An IEEE copyright form should accompany your final submission.

REFERENCES

[1] Road vehicles - Functional safety, ISO 26262, 2011.

[2] H. S. Mahajan, T. Bradley, and S. Pasricha, “Application of systems theoretic process analysis to a lane keeping assist system,” Rel. Eng. Syst. Safety, vol. 167, pp. 177–183, 2017.

[3] W. S. Lee, D. L. Grosh, F. A. Tillman, and C. H. Lie, “Fault tree analysis, methods, and application: A review,” IEEE Trans. Rel., vol. RE-34, no.3, pp. 194–203, Aug. 1985.

[4] K. L. Lu and Y. Y. Chen, “Safety-Oriented System Hardware Architecture Exploration in Compliance with ISO 26262,” Applied Sciences,2022.

[5] M. J. Elizebeth, S. Khastgir, I. Babaev, et al, “Comparison of FTA and Stpa Approaches: A Brake-by-Wire Case Study,” SSRN Electronic Journal,2023.

[6] Yang W, Yanwen L, Chunshu L, et al, “Analysis and application of functional safety based on modified FMEA method,” Intelligent Robot Systems IEEE, pp.98-103,2017.

[7] R. C. Rajasimha, V. Arjun and H. G. Chandrashekhar, “Supplemental FMEA for Monitoring and System Response of Electronic Power Steering Control System Functional Safety,” SAE Technical Paper ,2022.

[8] R. C. Yang, I. B. Utne, “Towards an online risk model for autonomous marine systems (AMS),” Ocean Engineering, vol.251,2022.

[9] H. H. Kim, “SW FMEA for ISO-26262 software development,” in Proc. Asia Pacific Software Eng. Conf., pp.19-22, 2014. DOI: 10.1109/APSEC.2014.85.

[10] A. Mallya, V. Pantelic, M. Adedjouma, M. Lawford, and A. Wassyng,“Using STPA in an ISO 26262 Compliant Process,” in Computer Safety, Reliability, and Security, ser. Lecture Notes in Computer Science, no. 9922, pp. 117–129 ,Sep. 2016.

[11] L. Junfeng, Z. Yunshuang, Z. Shuai, C. Chao, and D. Zhibin, “A research on SOTIF of LKA based on STPA,” in 2022 IEEE International Conference on Real-time Computing and Robotics (RCAR), pp.396–400, 2022.

[12] PEGASUS, “Scenario Description and Knowledge-Based Scenario Generation,” 2021.

[13] HAZOP Studies - Application Guide, IEC 61882,2016.

[14] System Analysis for Automotive Systems Engineering. Society of Automotive Engineers, SAE J2980,2018.

[15] G. Changsheng, Y. Xuezhu, S. Chengrui, “On ISO 26262 Compliance and Safety Assurance for Autonomous Vehicles using STPA,” Proceedings of the 2022 International Conference on Computer Science, Information Engineering and Digital Economy, pp.144-153, 2022.

[16] N. Leveson and J. Thomas, “STPA Handbook,” MIT Press, 2018.

[17] A. Mallya, V. Pantelic, M. Adedjouma, M. Lawford, and A. Wassyng “Using STPA in an ISO 26262 Compliant Process,” in Computer Safety, Reliability, and Security, ser. Lecture Notes in Computer Science, no. 9922, pp. 117–129, Sep. 2016.

AUTHOR INFORMATION

Lei He received the Ph.D. degree from Jilin University, Changchun, China, in 2011. He is currently an Associate Professor with the College of Automotive Engineering, Jilin University He is the author or coauthor of numerous publications in the field of environmental awareness and vehicle control, and is responsible for several state-funded intelligent driving modeling and simulation government projects.

Feng Ye is currently pursuing the M.S. degree in automotive engineering with the State Key Laboratory of Automotive Simulation and Control, Jilin University, Changchun, China. His research focuses on automotive intelligent driving functional safety and safety of the intended functionality.

Xiucai Zhang is currently pursuing the M.S. degree in automotive engineering with the State Key Laboratory of Automotive Simulation and Control, Jilin University, Changchun, China. His research interests are based on V2X infrastructure-side multi-target detection.

Zhongju Di received the M.S. degree from Harbin Institute of Technology University, Harbin, China. He is an intermediate engineer and currently works at China FAW Group Corporation. His research focuses on functional safety and safety of the intended functionality of automotive intelligent driving.