STPA-SysML based identification of expected functional safety hazards

1st Hong Li
China Intelligent and Connected Vehicles (Beijing) Research Institute Co
td. *Safety of the Intended Functionality Department, Beijing*
lihong@china-icv.cn

2nd Qidong Zhao
China Intelligent and Connected Vehicles (Beijing) Research Institute Co
td. Functional Safety Department, Beijing
zhaoqidong@china-icv.cn

3rd Yumeng Li
China Intelligent and Connected Vehicles (Beijing) Research Institute Co
td. Functional Safety Department, Beijing
liyumeng@china-icv.cn

Abstract—**The successful application of the advanced system modeling language SysML and the concepts of System Theoretical Process Analysis (STPA) in this study and the introduction of an innovative edge scene recognition algorithm have achieved so many significant recognition enhancement. Our work not only provides a more accurate means of recognizing expected functional safety, but also sheds light on further research in the field of system safety. Our approach provides engineers and researchers with a more efficient and reliable means of identifying potential security risks in systems, thus providing stronger support for system design and development.**

Keywords—Intelligent Driving; Intended Functional Safety; System Modeling Language; Hazard Analysis and Risk Assessment; Critical Hazard

I. INTRODUCTION

With the rapid development of the domestic automobile industry, the large-scale popularization of new energy vehicles has led to the penetration rate of cars with intelligent driving functions climbing year by year. By the University of Michigan Transportation Research Institute 2019 in a collaborative study, it was noted that L2 and L1 level autonomous driving has a significant effect in reducing traffic accidents. The study investigated the performance of 3.7 million vehicles over the period 2013-2017 and combined crash data from 10 U.S. states in its analysis. The study showed that the Emergency Braking System/Forward Collision Alert feature helped vehicles reduce rear-end crashes by 46 percent, the Lane Keeping Assist/Lane Departure Warning feature helped vehicles reduce crashes due to lane departure by 20 percent, and the Lane Change Alert System/Side Blind Zone Warning feature helped vehicles reduce crashes by 26 percent. However, as the traffic environment becomes more and more complex, safety problems caused by many random and unknown factors such as insufficient functions or performance limitations of hardware sensors, perception, decision-making, and control systems, unknown and uncertain dynamic characteristics of the actuating system, and misuse by personnel are gradually emerging.

According to the L2-level autonomous driving accident data report released by the U.S. National Highway Traffic Safety Administration last July, in the 10-month period from July 1, 2021 to May 15, 2022, there were 392 accidents related to L2-level ADS-assisted driving systems. Therefore, how to ensure the safe operation of intelligent driving systems in complex dynamic traffic environments is one of the core issues that need to be solved urgently to limit the large-scale technological landing and popularization and application of intelligent driving vehicles.

In order to address road vehicle safety, the International Organization for Standardization (ISO) released the international standard ISO 26262 "Functional Safety of Road Vehicles" in 2011[1] , and released an updated version in 2018.Functional safety aims to address the unreasonable safety risk due to the malfunctioning of the vehicle's electrical and electronic systems that lead to hazardous behaviors, but are unable to deal with hazards due to design inadequacies or performance limitations. Therefore, in order to address the safety issues specific to intelligent driving vehicles compared to traditional vehicles, international scholars have proposed the Safety of the Intended Functionality (SOTIF) concept.In February 2016, the International Organization for Standardization (International Organization for Standardization, ISO) under the Functional Safety Working Group (ISO/TC22/SC32/WG8) initiated the development of the international standard for Safety of the Intended Functionality, ISO 21448, and released the draft international standard for Safety of the Intended Functionality, ISO/PAS 21448, in January 2019 [2], and in December 2019 and November 2020 to form the draft ISO 21448 CD version and the draft ISO 21448 DIS version [3] , and the official ISO 21448 expected functional safety standard was released in June 2022 . The standard defines a standard process for the analysis, validation and verification of intended functional safety.

II. STATE OF THE ART OF RESEARCH ON THE SAFETY OF THE INTENDED FUNCTIONS OF INTELLIGENT DRIVING VEHICLES

Due to the continuous advancement of the SOTIF (System-on-Test in Functional Integration Flow) standardization process, governments, enterprises, and research institutes in China and internationally have achieved remarkable results in SOTIF practice solutions. In the field of product development, well-known companies such as BMW and Baidu have tried to integrate the SOTIF concept into the whole life cycle safety development process of their products in order to improve the safety performance of their products. In the area of product safety analysis and assessment, Continental, ANSYS and other companies have actively introduced safety analysis tools to identify and address potential safety risks more efficiently. At the same time, the EU's ENSEMBLE program and the U.S. NHTSA (National Highway Traffic Safety Administration) and other organizations have also carried out SOTIF analysis and assessment practices, and released reports on the results, providing valuable experience for the industry.

In terms of safety verification and validation, the EU's PEGASUS project and its extension projects VVM and SetLevel, as well as Japan's SAKURA project and the China Intelligent Networked Vehicle Alliance's Anticipated Functional Safety Working Group have combined SOTIF with related technologies in practice to ensure the safety performance of the products in practical applications. In terms of functional improvement, several companies have proposed targeted optimization solutions. Projects such as the EU's DENSE [4], on the other hand, have conducted in-depth research on the specific functional inadequacies of key components such as sensors, providing important support for improving overall system safety.

Adopting effective safety analysis techniques can improve the efficiency, comprehensiveness and scientificity of identifying and analyzing SOTIF hazards, potential functional deficiencies and triggering conditions. Traditional safety analysis techniques, such as fault tree analysis, failure mode and effect analysis, and hazard and operability analysis, have been used in some applications in SOTIF analysis and evaluation; new technologies represented by intelligent vehicles have brought new safety challenges such as changes in the nature of accidents, new types of hazards, reduction of the tolerance of single accidents, increase in the complexity of the system, and complexity of human-computer interaction, and so on, and therefore more effective safety analysis techniques are needed. As a result, there is a need for more effective safety analysis techniques. Systems-theoretic process analysis (STPA) has the potential to analyze complex systems, which consists of four steps: defining the purpose of the analysis, constructing a control structure, identifying unsafe control behaviors, and identifying causal scenarios, and it has been used in the SOTIF analysis of perception, decision-making, and fully automated driving systems, among others. However, the availability of a single technique is limited, and their individual strengths can be combined to develop more effective SOTIF analysis techniques [5].

The core idea of STPA is to interpret a hazardous event as a consequence of "unsafe control behavior" in the control loop due to a variety of possible causes, including, but not limited to - Localized failures: Failures due to false perceptions of the state of the environment or other components, inaccurate models of the external environment underlying the phenomena, Failures due to faulty perception of the state of the environment or other components, inaccurate models of the phenomena underlying the external environment, failure of interactions between subsystems (e.g., timing and arbitration conditions), feature interference, etc. At the same time, in addition to explicitly addressing human-computer interaction, STPA is unique from FMEA (Failure Mode and Effects Analysis) or similar techniques in that STPA is not limited to the technical parts of a technical system. That is, STPA can analyze misinterpretation of functionality, misleading alerts and signals of technical systems, human error and even intentional misuse, which are important parts of ADAS and autonomous driving systems [6].

SysML (System Modeling Language) is a graphical modeling language for a wide variety of systems and is recognized as an enabling technology for Model-Based Systems Engineering. The SysML standard from OMG states that "SysML supports the specification, analysis, design, verification, and validation of systems including hardware, software, data, people, programs, and facilities. The SysML standard at OMG states that "SysML supports the specification, analysis, design, verification, and validation of systems that include hardware, software, data, people, procedures, and facilities." The SysML standard defines a notation, not a methodology for using it. Therefore, SysML needs to be associated with a methodology supported by one or more tools.

There are a number of tools that can describe a model in SysML, some of which allow further model simulation and validation. These tools include Cameo Systems Modeler, Entreprise Architect, Modelio, Rhapsody, SCADE Architect, Papyrus, and Medini.Since SysML is not a methodology, and since the MBSE methodology relies on three elements (language, tool, method), it is necessary to relate the methodology to the tools used to develop the SysML model. Since SysML is not a methodology, and since MBSE methodologies rely on three elements (language, tool, methodology), it is necessary to relate the methodology to the tool used to develop the SysML model.A SysML tool is usually associated with a methodology that can be adapted to meet the methodology already in use by the company or organization deploying the tool.

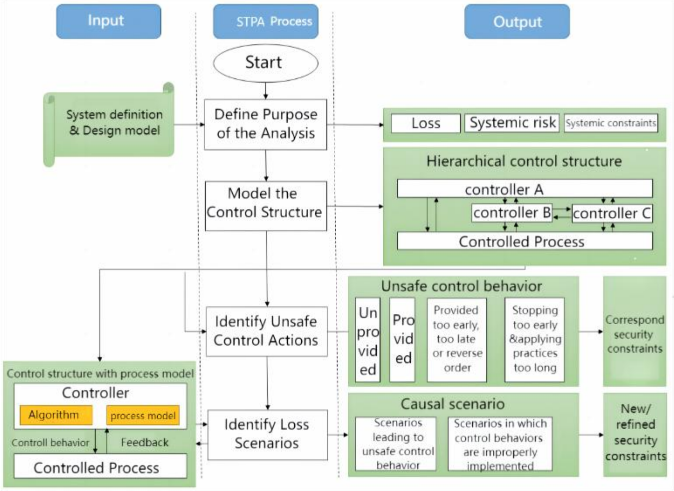
Input
STPA Process
Output
Start
System definition & Design model
Define Purpose of the Analysis
Loss
Systemic risk
Systemic constraints
Hierarchical control structure
controller A
controller B
controller C
Controlled Process
Model the Control Structure
Unsafe control behavior
Identify Unsafe Control Actions
Unprovided
Provided
Provided too early, too late or reverse order
Stopping too early &applying practices too long
Correspond security constraints
Control structure with process model
Controller
Algorithm
process model
Controll behavior
Feedback
Controlled Process
Identify Loss Scenarios
Causal scenario
Scenarios leading to unsafe control behavior
Scenarios in which control behaviors are improperly implemented
New/ refined security constraints

Fig. 1. STPA technology realization process

STPA-based SOTIF edge scene hazard identification can be used to construct a SOTIF risk protection technology system, so as to explore the system improvement ideas to reduce the SOTIF risk of the whole vehicle on the basis of theoretical research. Combined with the SOTIF hazard generation mechanism and risk model, we explore and optimize the functional improvement technology of each module of the intelligent vehicle, and further construct a vehicle-level SOTIF risk protection system with self-awareness and self-regulation capabilities. As shown in Figure 1-2, the internal state of the system (e.g., AI model), the external operating environment (e.g., ODD), and other constraints (e.g., traffic laws and regulations) are monitored, and then the adaptive safety decision model is designed to realize the protection against SOTIF risk.

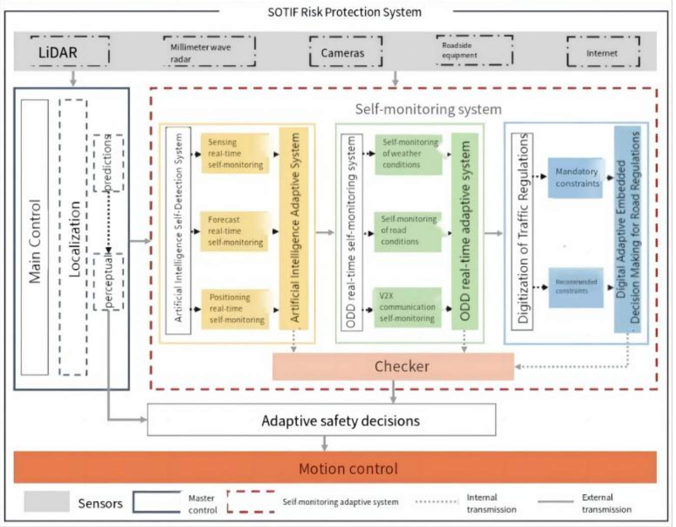
SOTIF Risk Protection System
LiDAR
Millimeter wave radar
Cameras
Roadside equipment
Internet
Self-monitoring system
Main Control
Localization
predictions
perceptual
Artificial Intelligence Self-Detection System
Sensing real-time self-monitoring
Forecast real-time self-monitoring
Positioning real-time self-monitoring
Artificial Intelligence Adaptive System
ODD real-time self-monitoring system
Self-monitoring of weather conditions
Self-monitoring of road conditions
V2X communication self-monitoring
ODD real-time adaptive system
Digitization of Traffic Regulations
Mandatory constraints
Recommended constraints
Digital Adaptive Embedded Decision Making for Road Regulations
Checker
Adaptive safety decisions
Motion control
Sensors
Master control
Self-monitoring adaptive system
Internal transmission
External transmission

Fig. 2 SOTIF Risk Protection System

To address the problem that the comprehensiveness of the STPA method is difficult to be guaranteed, this paper introduces a system modeling language (SysML) that encompasses the state of the vehicle and the operating environment of the self-driving system, and redefines the relevant terms of the hazard events, so that the model assumptions, requirements capture, and scenario construction can be used to determine the control structure and loss design that can be used to serve both the operating environment and the limitations of the self-driving system. Section 2 of this paper focuses on describing the STPA-SysMLbased hazard identification method, Section 3 shows the application of the method to an automatic lane keeping system for self-driving vehicles, and Section 4 concludes with a summary and outlook.

III. Methods for identifying safety hazards of intended functions of intelligent driving vehicles

A. Vehicle architecture and hierarchical scope

The subsequent analysis in this paper is based on intelligent networked vehicles with an L3 level of autonomous driving, where the vehicle has a certain ability to perceive and monitor information about its surroundings and complete driving tasks under specified environments and conditions. For the consideration of safety analysis, the driver's immediate takeover authority is also taken into account. On the basis of the traditional vehicle function of executing the driver's commands, the vehicle has complete automatic driving sub-functions, including: automatically slowing down or going around and pulling over when encountering roadblocks; cruising according to the specified route, such as constant speed and following cruise; smoothly passing through traffic lights or turning according to the guidance of the signal lights; smoothly changing lanes of the vehicle, i.e., according to the surrounding environmental data, roadway traffic efficiency and the reserved driving routes, judging whether it is necessary to change the current lane; autonomous parking; autonomous parking; and the ability to change the current lane according to the surrounding environment and conditions. The vehicle changes lanes smoothly, i.e. judging whether it needs to change the current lane according to the data of the surrounding environment, road traffic efficiency and the reserved driving route; Autonomous Parking function, including two ways of side parking and reverse parking.

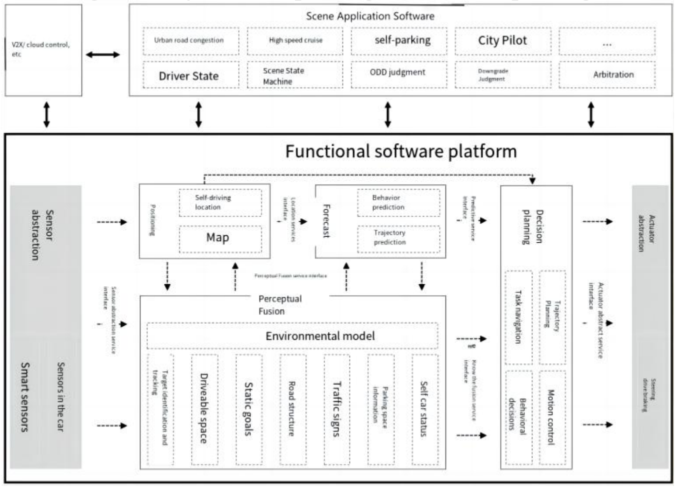

Fig. 3. Intelligent Driving Function Software Platform Architecture

In order to further improve the autonomous driving capability of intelligent networked vehicles, this paper introduces high-performance sensors and processors such as LIDAR, 4D millimeter-wave radar, and graphic processing chip on the basis of the original intelligent cockpit, camera, high-precision map, and ultrasonic radar. The addition of these devices and algorithmic components makes the car's accuracy in object detection, perception fusion and intelligent decision-making significantly improved. The intelligent connected car architecture designed in this paper is shown in Figure 3, and the whole is divided into perception layer, decision-making layer, control layer and execution layer.

At the execution layer, intelligent networked vehicles, relying on strong hardware support, can quickly transform the instructions of the control layer into actual actions, realizing the automatic driving of the vehicle. In addition, the execution layer will adjust its behavior according to the real-time feedback data to adapt to the ever-changing external environment.The smart connected car architecture designed in this paper has strong coupling and flexibility at all levels, and is able to cope with various complex autonomous driving scenarios.

Our approach is to extend the existing risk assessment methodology used by ISO 26262 practitioners to include multiple models. According to the ISO 26262 methodology, risk is assessed by the severity of the hazard, S, the exposure, E, and the controllability, C. The risk of a hazard is assessed by the severity of the hazard, E, and the controllability, C. In practice, the value of S can be limited to property damage or injury or death; the relative frequency of injuries is shown in Table I

Table I. Relative frequency of injury types

Crash Severity	Crash Incidents	% of Injuries	K Person injures	K Person injures	K Person injures	K Person injures	O Prop Damage
K= Fatality	4502	1.8	4901	1353	1284	1027	2357
A=Sever Injury	33247	13.0	0	39711	7696	7976	26668
B=Major Injury	62474	24.5	0	0	74811	12247	66451
C=Minor Injury	39222	15.4	0	0	0	55767	52985
O=No Injury/PDO	115451	45.3	0	0	0	0	261971
Total	254896	100	4901	41064	83791	77017	410432

The severity E can have a value of 0 < E < 1, representing the probability of the hazard occurring.C can have a value of 0 < C < 1, whereby C = 1 means that the vehicle cannot avoid the hazard (e.g., it will definitely crash), and C = 0 means that the hazard can always be avoided (e.g., it will always fail to crash). With this approach, hazards are grouped according to their severity. The hazards in each group are denoted as $\mathcal{H}$ and the corresponding risk R_H is available for each hazard with $H \in \mathcal{H}$, where the equation is $R_H = E_H \times C_H$:

$$\begin{cases} H \in \mathcal{H}_{pdo} \quad if\ S_H = "property\ damage\ only" \\ H \in \mathcal{H}_{injury} \qquad if\ S_H = \text{"injury"} \\ H \in \mathcal{H}_{fatality} \qquad if\ S_H = \text{"fatality"} \end{cases} \tag{2}$$

Unlike ISO 26262, where the hazard represents a single vehicle failure, assessing the residual risk associated with autonomous driving requires consideration of hazards where multiple vehicles are present in a given situation.

Example 1: To illustrate the different categories, consider the data obtained from Table 30, based on the 2010 MAIS and KABACO data, as shown in Figure 7, where we observe that less than 2% of crashes result in fatal injuries i.e., Fatal Hazards $\mathcal{H}_{fatality}$, and almost half result in property damage only i.e $\mathcal{H}_{pdo}$, Medium Hazards. The remaining half are associated with multiple injuries i.e. $\mathcal{H}_{injury}$.

For a collection of disjointed hazards $\mathcal{H}_i$, the overall relevant residual risk can be estimated as the sum of the individual residual risks. However, when hazards are superimposed, their severity, exposure and controllability need to be assessed. For simplicity, it is reasonable to assume that the severity of a superimposed hazard is equal to the maximum severity of each of its components. The overall residual risk for each severity type ("property damage", "injury", "death") H=$\{h_1, ..., h_n\} \sqsubset \mathcal{H}$ will be expressed as a possible superimposed hazard:

$$R_{\mathcal{H}} = \sum_{\forall H \sqsubset \mathcal{H}} E_{\mathrm{H}} \times C_H \tag{2}$$

Given that there are 2^n subsets in the n-hazard set $\mathcal{H}_i$, the exponential complexity makes the Eq. calculation impractical. It is therefore necessary to propose an efficient evaluation that does not need to explicitly consider all possible subsets.

B. Boundary risk

In the case where$R_{\mathcal{H}} = E_{\mathrm{H}} \times C_H$ and C are both between 0~ 1, $R_H \leq E_H$and $R_H \leq C_H$ are significant. Thus, a notable way to provide an upper bound on R_H is to obtain an upper bound on E_H or C_H. We assume that hazards are unavoidable and use C = 1 to further simplify the scope of superimposed risk by defining superimposed risk in terms of the joint probability of all hazards in $H \sqsubset \mathcal{H}$, i.e.

$$R_{\mathcal{H}} = R_{h_1,\ldots,h_n} \leq P(h_1, \ldots, h_n) \tag{3}$$

This simplification allows the risk to be bounded by estimating the probability density associated with the occurrence of any subset of risks in $\mathcal{H}_i$. More rigorously, for each individual hazard $h \in \mathcal{H}$, the total risk $R_{\mathcal{H}}$is bounded by the sum of the probabilities of independent occurrences and the probabilities of their superposition with any other subset of HI, i.e.

$$R_h \leq \sum_{\forall H \sqsubset \mathcal{H}} P(h \cup H) \tag{4}$$

To avoid considering combinations of hazards that are unlikely to be superimposed, $\mathcal{H}_i$can be divided into k clusters $C_1, \ldots., C_k$ such that the probability of superimposing hazards in different clusters is low, i.e:

$$h_i \in C_i, h_j \in C_j \rightarrow P\left(h_i, h_j\right) \ll \min\left(P(h_i), P(h_i)\right) \tag{5}$$

For these clusters, the complexity of computing the residual risk is linearly related to the number of clusters, but approximates an exponential decrease with the size of the cluster:

$$R_h \leq \sum_{i=1}^{k} R_{c_i} \leq \sum_{i=1}^{k} 2^{|C_i|} \underbrace{max}_{\forall h \in C_i} P(h) \tag{6}$$

The bounds can be made tighter by modeling the conditional probability and causality of superimposed hazards, e.g., using probabilistic causal models. The polynomial complexity of Bayesian inference, on the other hand, can be handled by mapping clusters to buckets and applying pinning terms.

IV. EXAMPLES OF PERSONNEL MISUSE SAFETY ANALYSIS

A. Driving rights switching study

During the operation of the self-driving car, the self-driving system will continuously receive situational information from all directions, including dynamic and static ODD, the vehicle's own operating status and driver status information. According to the current received contextual information, the autonomous driving system will conduct a comprehensive analysis and make corresponding decisions. However, real-world traffic scenarios are complex and changeable, and the autonomous driving system may encounter various unexpected situations, such as system failure, vehicle out of the operational design domain, poor driver status, etc. At this time, the system is unable to make a decision, and then it will send out a takeover signal to remind the driver to take over the Dynamic Driving Task (DDT) in a timely manner.

Several studies have shown that the success of the driving authority switchover is highly dependent on the specific automation function, traffic conditions, and task description. For L3 and above, the entire dynamic driving task is assumed by the driving automation system within the operational design domain, and an example of a takeover can be seen in Fig. 4. The Automated Driving System (ADS) may continue to execute the DDT for at least a few seconds after providing the takeover-ready user with a request to intervene. Subsequently, the DDT takeover-ready user shall resume execution of the DDT or achieve a minimum risk condition if deemed necessary.

In L4 and L5 driving automation systems, the autopilot system must have the ability to perform a DDT takeover with minimal risk conditions. In the case of the L4 driving automation DDT takeover ,the autopilot system operates normally until an ADS system failure occurs, and the failure does not affect the ADS from continuing to perform DDT performance.

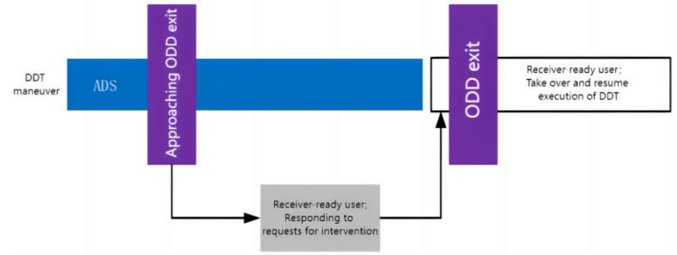
DDT maneuver
ADS
Approaching ODD exit
ODD exit
Receiver-ready user; Take over and resume execution of DDT
Receiver-ready user; Responding to requests for intervention

Fig. 4. L3 Level Driving Automation DDT Takeover

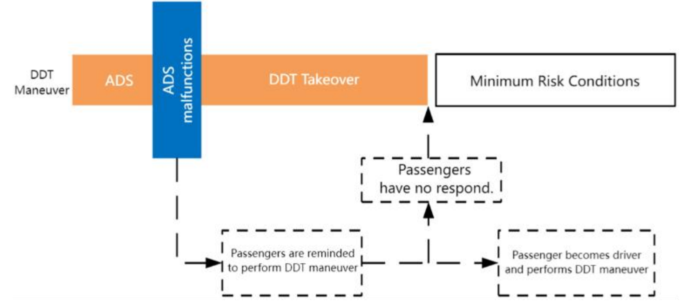
DDT Maneuver
ADS
ADS malfunctions
DDT Takeover
Minimum Risk Conditions
Passengers have no respond.
Passengers are reminded to perform DDT maneuver
Passenger becomes driver and performs DDT maneuver

Fig. 5. L4 Level Driving Automation DDT Takeover

B. *Human factors characterization*

Based on existing autonomous driving technologies, it is foreseen that "semi-autonomous" vehicles, driven by both autonomous driving systems and human drivers, will constitute the majority of vehicles for some time to come. From a human factors perspective, a fundamental issue for semi-autonomous vehicles is how to design human-computer interaction systems so that the driver is fully aware of the vehicle's capabilities and limitations, and maintains situational awareness of what the vehicle is doing and when human intervention is required.

Previous human factors research has shown that automation addresses the imprecision and variability of manual task performance, but it also creates new types of safety problems. High levels of automation can lead to out-of-the-loop problems such as human overconfidence, skill degradation, distraction (when automation operates reliably), mental overload (when operators suddenly need to solve automation-induced problems), and loss of situational awareness [9][10][11][12], which also pertain to the field of autonomous driving [13][14]. These studies demonstrate the need for researchers, designers and policy makers to carefully consider human factors [15]. This section examines and summarizes the human factors in HCI systems that affect the safety of autonomous driving.

(1) Cognitive properties

Recognizing and understanding the current traffic environment is a prerequisite for drivers to achieve safe driving, and situational cognition is also considered to be one of the most important human factors for achieving driving safety. The cognitive characteristics of drivers in human-machine co-driving environments are mainly characterized by low attention levels, lack of gaze, and the lack of sufficient time before control switching, limited access to information for drivers, and resulting in a lag in the speed of situational understanding; questionnaire surveys have shown that perceptual and cognitive trust and perceptual safety affect the behavior of drivers of intelligent vehicles, and are also factors affecting the use of self-driving cars [17]. .

(2) Driving load characteristics

The driving load in the human-machine co-driving environment is quite different from that of traditional manual driving, mainly in terms of underload (when the automatic system is working) and overload (when the person is suddenly asked to take over the driving). When driving manually, the human is allowed not to monitor the environment outside the vehicle in real time, and the brain and cognitive loads are at a lower level; while in unexpected or complex situations, when the human is suddenly asked to take over the control of the vehicle, there is a surge in the brain and cognitive load demand, and this kind of jumping from very low to very high degree of the driving load characteristics has a direct impact on the safety of the switching process. Studies have shown that when driving load decreases, drivers are more inclined to engage in other tasks rather than supervise the autopilot system [18]. In view of this, some scholars have begun to study the effect of subtasks on takeover performance, hoping to improve takeover performance by enhancing the driver's available attentional resources with the load demand of subtasks.Louw et al [19] found that engaging in subtasks may weaken the driver's situational cognitive ability and thus reduce driving performance compared with manual driving through simulated driving experiments.Neubauer et al [20] simulation experiments showed that subtasks can have a positive impact on improving takeover performance by maintaining a certain level of brain load for the driver compared to driving under automated driving.

(3) Reaction characteristics

When a switch in control occurs, the driver's reactive force is the driver's ability to resume looking ahead and operate the vehicle in a timely manner after receiving a takeover request from the system. Reactivity is mainly quantified by a variety of reaction times (e.g., the time from the takeover request from the system to the time when the driver first looks ahead or touches the steering wheel) and takeover times (the time from the takeover request from the system to the time when the driver operates the steering wheel or pedals to achieve manual driving).

Driver reactivity is closely related to cognitive ability, with lower cognitive levels implying longer reaction times and takeover times. Driver reaction in automatic driving state is significantly lagged than in manual driving, especially when the driver is engaged in sub-tasks that require the use of eyes [21]. There is no uniformity in driver reactivity characteristics because the influencing factors are diverse and closely related not only to the type of takeover event, but also to the environment in which the driver is located (type of road, density of traffic flow, weather, etc.) as well as the driver's state (sub-tasks engaged in, eye-movement behavior, etc.).

C. Classification of control switches

Autopilot takeover function is essentially a driving right switching problem, according to the different initiators and executors of driving right switching, it can be categorized as initiated by the driver and initiated by the driving automation system. [2] , as shown in Table I

TableI: Literature [2] Driving Rights Conversion Classification

initiator	Vesting of driving rights		define	give an example
	pre-initiation	post-launch		
pilot	pilot	systems	activation	The driver hands over the controls to the system
	systems	pilot	interventions	Driver-initiated maneuvering
systems	systems	pilot	receivership	The system is manipulating the driving privileges, the system realizes that it is not capable and requests a handover to the driver
	systems	support system	Activating the Minimum Risk Strategy	Systematic adoption of risk reduction measures

For broad control switching, it can be categorized into human-initiated optional switching, human-initiated mandatory switching, and system-initiated mandatory switching based on the initiator and mandatory nature of the switching [6] As shown in Table II

Table II: Literature [6] Driving Rights Conversion Classification

initiator	typology	driving license	give an example
man	optional	People and systems	Produced by the driver actively turning the system on or off in a non-emergency situation.
man	compulsory	man	The driver realizes that the system is not up to the task of driving and actively takes over control.
		systems	When a driver finds himself/herself unable to perform driving duties for physical or psychological reasons.
systems	compulsory	man	The system finds itself unable to perform the driving task and requests the driver to take over.
		systems	A switchover initiated by the system when it realizes that the driver who is driving is incapable of performing the driving task.

The SAEJ3016 standard, in its description of the roles of the person and the system under Level L3 automated driving, states that the person should take over control within a certain period of time after receiving a request, and that the system should only be disabled if the request is made and after waiting for the person to take over safely [7] Therefore, the switching of control in the human-machine co-driving environment refers more specifically to the switching from the system to the human, i.e., the switching in the narrow sense. It involves a lot of scenarios, and requires high requirements on the driver's state and takeover ability, which is a difficult point of control switching. Switching from system to driver can be divided into five scenarios as shown in Table III according to the planning and initiator of switching.

Table III System-to-driver driving authority switching

typology	give an example
System-initiated scheduled switchover	For example, the system sends a takeover request at the appropriate time before it is about to enter a section of road known to be unsuitable for automated driving (e.g., entering an on-ramp, construction zone).
System-initiated unscheduled switchover	For example,a sudden change in road conditions (e.g., lane lines disappearing) or a driving environment that it is beyond the scope of the system's function and the system temporarily requests to take over.
Unscheduled switchover initiated by a person	For example, if a person takes over the system for the pleasure of driving, or if he or she does not trust the system.
Unscheduled switchover initiated by a person on an emergency basis	The person discovers emergencies that the system didn't pick up on and takes over proactively.
Unscheduled switchover initiated by system emergency	System internal function error or module failure, inform the driver to take over the control urgently

Whether driving manually or automatically, the driver is the central factor playing a dominant role in the coordination and control of the system elements. Therefore, the driver's cognitive-response model of driving authority takeover is human-centered [8]. When the system takes over, the driver's cognitive-response behavior can be divided into three stages: (1) perception: detecting the surrounding car and identifying the vehicle condition; (2) judgment: filtering, analyzing and processing the acquired information, and making the corresponding decisions; (3) response: implementing the corresponding response behavior. Any error in this process can lead to personnel misuse and traffic accidents. By analyzing the driver's cognitive response stage and the influence factors of automatic driving takeover, the cognitive correspondence model of automatic driving takeover can be established, as shown in Figure 3-3. The model is divided into three stages, in the perception stage, the driver receives external information through eyes, ears and other senses. The external information includes vehicle factors and scene factors. In the judgment stage, sensory memory is transferred to the central nervous system over sensation, which is converted into working memory supplemented by the long term memory generated by the autopilot training, enabling the driver to recognize, judge and decide. In the response stage, the information after judgment and decision is transmitted to the human operating organs, producing actions such as adjusting the takeover posture, controlling the direction, and controlling the speed. The model suggests that driving takeover is a process of continuous adjustment and correction cycle, in which the causes of human error cannot be analyzed in isolation but should be explored from a spatial-temporal multidimensional perspective and explored through empirical research.

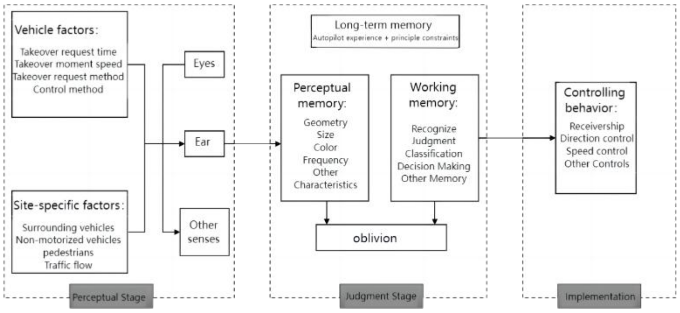

Figure 6 Autopilot takeover cognitive model

V. Examples of personnel misuse security analysis

Potentially hazardous events in vehicles resulting from personnel misuse should be identified and risk assessed, and if it is demonstrated that these potentially hazardous events do not result in an unreasonable risk of injury, then no specialized measures are required to ensure the intended functional safety. Hazards are potential sources of injury and result from risky behavior at the whole vehicle level, and the inability to adequately control hazardous events is a contributing factor to injury, and Figure 3-4 illustrates the reasons why hazardous events are not controlled.

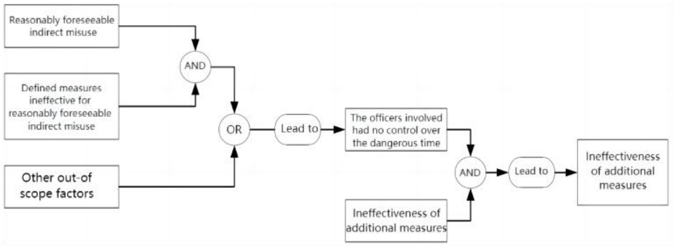
Reasonably foreseeable indirect misuse
Defined measures ineffective for reasonably foreseeable indirect misuse
Other out-of scope factors
AND
OR
Lead to
The officers involved had no control over the dangerous time
Ineffectiveness of additional measures
AND
Lead to
Ineffectiveness of additional measures

Figure 7 Reasons for Uncontrolled Hazardous Events

This section is carried out under the guidance of ISO 21448 standard to explore the SOTIF test and evaluation method of HMI system by taking the human-computer interaction of Automated Lane Keeping Systems (ALKS) as an example. Firstly, in the safety analysis phase, the performance limitations and trigger conditions of the HMI system are analyzed in combination with the STPA method, which serves as the basis for the subsequent test and validation phase; secondly, the safety performance evaluation system of the expected functions of the HMI system is constructed; and lastly, the test and evaluation method and functional modifications of the HMI system are summarized and introduced.

ALKS belongs to the L3 level of conditional autonomous driving on structured roads approximating highways (e.g., urban expressways, etc.) with a speed range of 0-60km/h. Upon activation, the system continuously controls the vehicle horizontally and vertically and is responsible for the execution of the Object and Event Detection and Response task (OEDR:Object and Event Detection and Response). The behavior considering only the presence of interaction between the driver and the system is shown in Table IV.

Table IV: Driver Interaction Functions

interactive function	Functional Description
Activate/deactivate the system	Drivers can activate or deactivate the system via function buttons on the steering wheel or other locations
Setting navigation destinations	After the driver turns on the system in the ODD, he/she needs to assign a destination to the ALKS system, and the ALKS navigation system will generate a path, according to which the self-driving vehicle will drive to the designated place and complete the self-driving task
Setting the cruise speed	After turning on the system, the driver can set the cruise speed so that the vehicle will drive at the preset cruise speed
Setting the following distance	After turning on the system, the driver can set the following distance so that the vehicle will follow the preset following distance.
Maneuvering vehicles	The driver needs to steer the vehicle with the steering wheel, brake and accelerator pedals during manual driving; during automatic driving, the driver can override the automatic driving system by using the pedals or the steering wheel for short periods of time.
receivership	When ALKS experiences a system failure or goes out of the operational design domain, the system sends a takeover request to the driver, who needs to take over control of the vehicle
Interaction with other vehicle components	Driver interactions with other components include fastening seat belts, opening and closing doors, leaving the driver's seat, center control system settings, toggling steering levers, etc.

The working principle of ALKS system is as follows: each sensing sensor obtains information about the surrounding environment, traffic flow, obstacles, road signs, and vehicle status, etc. The information is transmitted to the domain controller of the ALKS system, which understands and processes the information through the sensing fusion, planning, and control modules, and then outputs the control of the vehicle's steering, braking, and power execution systems to ultimately realize the execution of the dynamic driving task. According to the above functional definition of ALKS system and the initial configuration scheme of the system, the initial architecture of the system is obtained.

STPA-based safety analysis

STPA Step 1: Define the purpose of the analysis

(1) Defining potential accidents

Table Ⅳ: List of Accidents

serial number	incident
A-1	Loss of life or injury to driver and passengers or other persons
A-2	Damage to vehicles and objects external to vehicles
A-3	Autopilot Mission Failed
A-4	Loss of user satisfaction and confidence in self-driving cars will not result in personal injury or property damage
serial number	Vehicle-level hazards
H-1	Collision of self-driving car with other vehicles, objects [A-1, A-2, A-3, A-4]
H-2	Self-driving car deviating from a pre-determined route [A-3, A-4]

H-3	Failure of self-driving cars to follow traffic regulations [A-3, A-4]

(2) Identify system-level hazards

Table V: System-level security constraints

STPA Step 2: Create a block diagram of the control structure

Create a block diagram of the ALKS system control structure, based on the relevant ALKS item definitions. The control structure block diagram summarizes how the execution of commands takes place without regard to the complete internal functioning of the individual components involved. The control structure block diagram includes the driver, the ALKS system (sensors, domain controllers, actuators, and HMI), and the external environment. In the control structure block diagram, feedback is indicated by blue arrows and control behavior is indicated by red arrows.

serial number	safety constraint
SC-1	Self-driving cars must prevent collisions between themselves and other vehicles or objects
SC-2	Self-driving cars must follow pre-determined routes
SC-3	Self-driving cars must follow relevant laws and regulations

STPA Step 3: Identify unsafe control behaviors

The unsafe control behaviors identified through the STPA primer are shown in Table VI.

Table VI. Unsafe Control Behaviors

Controlling behavior	Failure to provide control over the harm caused by the behavior	Harm caused by the act of providing control	Provide control of behavioral advancement, delay or sequential errors	Providing control over behavior that stops too soon or lasts too long
Open the system	UCA-1: When the ALKS system is available, the driver wants the ALKS system to assume the driving task without turning on the autopilot system. [H-3]	UCA-2: The driver turns on the autopilot system when the roadway environmental conditions are not suitable for turning on the ALKS system. [H-1]	UCA-3: Driver's ability to turn on ALKS system control of the vehicle is relinquished prior to the unification, which would put the vehicle at risk of a collision. [H-1]	N/A
Shut down the system	UCA-4: The driver failed to turn off the autopilot system when the roadway environmental conditions were no longer suitable for continued operation of the ALKS system. [H-1] UCA-5: The driver failed to turn off the autopilot system when the AKLS system completed the driving task. [H-3]	UCA-6: When the vehicle was in the path of a collision, ALKS was running and the driver turned off the autopilot system but did not resume manual control. [H-1]	UCA-7: The driver turned off the autopilot system too late when roadway environmental conditions were no longer suitable for continued operation of the ALKS system. [H-1]	N/A
Maneuvering vehicles	UCA-8: The driver did not maneuver the vehicle when the ALKS system was not available. [H-1] Example 1: A driver is driving manually when the vehicle in front of him slows down, and in order to avoid a collision, the driver fails to apply the brakes. Example 2: The driver was driving manually when the driver was traveling ahead to a curved road and the driver did not steer to drive. Example 3: When the autopilot system is not available, the vehicle speed exceeds the limit and the driver does not press the brake pedal	UCA-9: The driver executed an inadequate driving maneuver when the ALKS system was unavailable. [H-1] Example 1: A driver is driving manually to park in a parking lot, and the driver tries to slow down by pressing the brake pedal, but instead presses the accelerator pedal. Example 2: A driver traveling to a curved road makes a turn at a very high speed. Example 3: Vehicle speed exceeds the limit The brake pedal depressed by the driver does not Enough.	UCA-10: Performing driving maneuvers on a vehicle too late in some cases when the ALKS system is not available. [H-1] Example 1: During manual driving, the vehicle in front of you slows down and the driver brakes too late in order to avoid a collision.	UCA-11: When the AKLS system was unavailable, in some cases the driver stopped performing driving maneuvers too early. [H-1] Example 1: Vehicle ahead slows down and brakes stop too soon. UCA-12: Driver maneuvering vehicle too long while autopilot system is operating. [H-3]
override	N/A	UCA-13: While the autopilot system was performing a task, the driver wanted to accelerate the pedal override system to overtake the vehicle in front of him and stepped on the brake pedal. [H-1] UCA-14: Driver inadvertently triggers steering override by mistake when there is a vehicle in the adjacent lane. (In hazardous scenarios, driver mistakenly triggers reversible active intervention) [H-1]	N/A	UCA-15: The driver accelerates the override system for too long, exceeding the threshold, causing the system longitudinal control to exit and the driver to relinquish longitudinal control of the vehicle. [H-1] (driver triggers irreversible active intervention without subsequently providing control)
receivership	UCA-16: The driver did not take over maneuvering the vehicle when the	N/A	UCA-17: When the autopilot system sends	UCA-18: When the autopilot system sends

	autopilot system sent a takeover request. [h-1] [h-2] [h-3]		a takeover request, the driver takes over maneuvering the vehicle too late. [h-1] [h-2] [h-3]	a takeover request, the driver fails to provide a sustained takeover maneuver, leaving the vehicle in an out-of-control condition. [h-1][h-2][h-3]
Setting navigation destinations	UCA-19: When the driver wants to use the autopilot system to reach a destination, the navigation destination information is not set. [H-3]	UCA-20: Driver sets navigation destination information outside the ODD or in hazardous scenarios. [H-3] UCA-21: Setting the navigation destination information outside the ODD at the touch screen when the driver wants to use the autopilot system to reach the destination. [H-3]	UCA-22: Driver sets navigation destination information at the touch screen before turning on the autopilot system. [H-3]	UCA-23: Driver has not yet reached the set destination with the autopilot system running and the driver has turned off the navigation destination information. [h-1] [h-3]
Setting the cruise speed	UCA-24: Cruise speed was not set after the driver turned on the autopilot system. [H-1][H-3]	UCA-25: The driver set a cruise speed in excess of the allowable range during operation of the autopilot system. [H-1][H-3] UCA-26: During autopilot, the vehicle ahead decelerates while the driver increases the cruising speed. [H-1]	N/A	UCA-27: When the autopilot system is available, the driver continuously presses and holds the increase/decrease cruise speed button. [H-1][H-3]
Setting the following distance	UCA-28: Driver failed to set the following hourly distance after turning on the autopilot system. [H-3]	UCA-29: Driver set too small a following time distance during autopilot operation. [H-1][H-3] UCA-30: During autopilot, the following vehicle decelerates and the driver reduces the time distance between following vehicles. [H-1]	N/A	UCA-31: When the autopilot system is available, the driver continuously presses and holds the increase/decrease following distance button. [H-1][H-3]
Buckle up, get out of the driver's seat, close the door, honk the horn, turn on the turn signal, turn on the windshield wipers, etc.	UCA-32: Driver was not wearing a seat belt while driving manually or while using the ALKS system. [H-3] UCA-33: Driver failed to close door while using ALKS system. [H-3] UCA-34: Driver failed to turn on turn signal while turning at intersection. [H-3] UCA-35: Driver failed to turn on windshield wipers while driving in the rain. [H-3] UCA-36: Failure of a driver to honk while passing through an intersection with no visual field. UCA-37: Driver failed to turn off turn signal after completion of turn. [H-3]	UCA-38: Driver unbuckling a seat belt while the driver is driving manually or while the vehicle is being driven automatically. [H-3] UCA-39: Vehicle on autopilot with driver out of driver's seat. [H-3] UCA-40: Driver opening door during vehicle autopilot. [H-3] UCA-41: Driver sleeping during vehicle autopilot. [H-3] UCA-42: Driver turns on windshield wipers in clear weather (interferes with driving visibility) [H-3] UCA-43: Drivers honked their horns frequently while using the ALKS system. [H-3] UCA-44: Driver turning on turn signal without turning while traveling in a straight line. [H-3]	UCA-45: Driver turns on turn signal too late when turning at intersection. [H-3]	UCA-46: Driver persistently honking horn, affecting attention of drivers of other vehicles. [H-3]

Table VII. Example of Potentially Hazardous Event Identification

Unsafe control behavior	Vehicle-level hazards	operating scenario		Potentially hazardous event
		take	traffic participant	
Driver does not take over maneuvering the vehicle when the autopilot system sends a takeover request	Failure to maintain a minimum safe distance between self-driving cars and obstacles such as other vehicles, objects and terrain	urban expressway	Accident vehicle ahead	The self-driving car traveling on an urban expressway encounters an accident vehicle in front of it, and the self-driving system sends a request to take over, and the driver fails to do so
ALKS is running and the driver turns off the autopilot system but does not resume manual control	Self-driving cars are out of control	urban expressway	Motor vehicles in adjacent lanes	Normal operation of a self-driving car traveling on an urban expressway where the driver turned off the self-driving system and did not resume manual control
Driver was driving manually to park in a parking lot and the driver tried to slow down by pressing the brake pedal but instead pressed the accelerator pedal	Collisions between self-driving cars and obstacles such as other vehicles, objects and terrain	Close to the lake parking lot	Other vehicles in the parking lot	The parking lot was near a lake and the driver went to park and tried to hit the brake pedal to slow down, but instead hit the gas pedal
The driver steers the override system for longer than	Self-driving cars are out of control	urban expressway	Motor vehicles in adjacent	When a self-driving car traveling on an urban expressway performs a driving task, the driver

permissible, causing the system to quit maneuvering the vehicle after automatic exit			lanes	overrides the control for too long causing the system to exit automatically, but then provides no control

Table VIII: Example of a risk assessment

Potentially hazardous event	potential consequence	severity		controllability		Acceptability of risk
		score (of student's work)	clarification	score (of student's work)	clarification	
The self-driving car traveling on city road/city expressway meets an accident vehicle in front of it and needs to take over, the self-driving system sends a request to take over, and the driver fails to take over.	Collision with an accident vehicle	S > 0	High vehicle speeds, high collision relative to vehicle speeds	C > 0	Failure of drivers to take over vehicles	N
Normal operation of a self-driving car traveling on a city road/urban expressway where the driver turned off the self-driving system and did not resume manual control	Collision with vehicle in adjacent lane	S > 0	High vehicle speeds, high collision relative to vehicle speeds	C > 0	Driver did not resume manual control	N
The parking lot was near a lake and the driver went to park and tried to hit the brake pedal to slow down, but instead hit the gas pedal	The car went into the lake.	S > 0	The driver had a hard time saving himself when he went into the lake.	C > 0	The driver didn't have time to react.	N
Driving tasks performed by self-driving cars traveling on urban roads/urban expressways where the driver overrides the control for too long resulting in the system automatically quitting without providing subsequent control	Collision with vehicle in adjacent lane	S > 0	High vehicle speeds, high collision relative to vehicle speeds	C > 0	The driver didn't have time to react.	N

Table IX: Detailed causal scenarios for UCA-1

Unsafe control behavior	Reasons for misuse		Causal scenario
	course of events	lead-in word	
UCA-1: When the driver wants the autopilot system to assume the driving task, but does not turn on the autopilot system. [H-3]	recognize	incomprehension	Drivers don't know where the button to turn on the autopilot system is located
			Drivers do not understand the system status displayed by the HMI
		misidentification	Driver misrecognizes the button to turn on the system
			The HMI system displays the wrong system status and the driver sees the HMI system status is on. (System not on but system status shows on)
	judgements	misjudge	Driver's button to confuse the on system and other function buttons
			Driver recognizes other states of the HMI display system as system on.
	gestion	misbehave	The driver wants to turn on the autopilot system, but the driver is distracted by pressing the wrong button.
		Intentional enforcement	Driver intentionally leaves autopilot on
		incapable	The driver doesn't know how to turn on the autopilot system the first time he or she uses the system.
			Button to turn on autopilot system is difficult to use
			Poor physical condition of drivers

Table X: Detailed Causal Scenarios for UCA-6

Unsafe control behavior	Reasons for misuse		Causal scenario
	course of events	lead-in word	
UCA-6: When the vehicle is in the path of a collision and the autopilot system is operating, the driver turns off the autopilot system but does not resume manual control. [H-1]	recognize	incomprehension	Driver fails to notice system off status display
			Although the driver turns off the autopilot system, the driver does not understand the system shutdown indication signal and does not know that the system has been shut down
		misidentification	(Driver turns off the autopilot system, but the system status display is not updated and the driver thinks the system is not turned off)
	judgements	misjudge	The driver turns off the autopilot system, but the system status display is not updated and the driver thinks the system is not turned off
	gestion	misbehave	Driver's poor mental state and misuse of the autopilot system to turn it off
			Drivers incorrectly interacting with the underlying system and unintentionally shutting it down
		Intentional enforcement	During the operation of the autopilot system, the driver intentionally operates the
		incapable	Driver presses other function buttons and accidentally presses the system off button
			Poor physical condition of drivers

STPA Step 4:Hazardous event identification

Regarding the identification of potential hazardous events due to unsafe driver control behaviors, the results of the identification of potential hazardous events are shown in Table VII below, using the driver taking over the vehicle, turning off the ALKS system, maneuvering the vehicle, and overriding the autopilot system interaction functions as examples.

STPA Step 5:Risk assessment

Potentially hazardous events in the vehicle resulting from unsafe control behaviors of the driver should be identified and risk assessed, and if it is demonstrated that these potentially hazardous events do not result in an unreasonable risk of injury, then no special measures are required to ensure the safety of the intended function. Using the potentially hazardous events in Table VII as an example, the results of the risk assessment are shown in TableVIII below.

STPA Step 6: Identification of causal scenarios

Once the risk has been determined to be unacceptable, the next step is to identify possible causal scenarios for the UCA. For each UCA, there are many possible causal scenarios. In this section, two typical unsafe control behaviors are selected for causal scenario identification. Taking UCA-1: When the driver wants the autopilot system to take on the driving task but does not turn on the autopilot system and UCA-6: When the vehicle is in the collision path and the autopilot system is running and the driver turns off the autopilot system but does not resume manual control as examples, the detailed causation scenarios are shown in Tables IX and X.

Combined with the above example of STPA analysis of personnel misuse, we use the SysML model of graphical elements for formal validation to organically integrate the ALKS system of the intelligent driving vehicle with the external environment, and form the process and functional transformation of the SOTIF software as shown in Figures 8. Based on the conversion model in the following figure, when identifying potential hazardous events, only the combination of the current vehicle state and the input environmental conditions, i.e., the semantic level of the functional scenarios, can be combined with the natural driving data and other related information to determine the parameters of the current vehicle state and the input environmental conditions and the parameter ranges, and then generate the logical scenarios as well as specific scenarios, which can be used to test and verify the above hazardous events and causative scenarios.

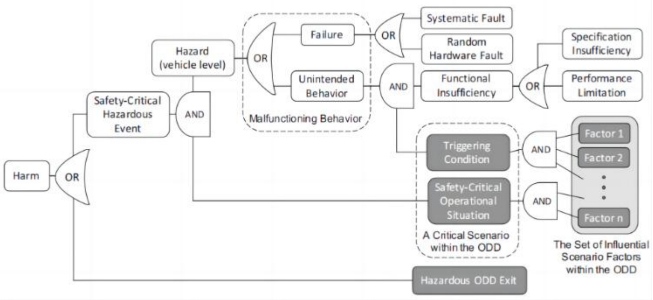

Figure.8.FTA Flowchart for Hazard Analysis

Table XI. Example of a Comparative Assessment of Three Approaches

Result	Old methodology	Baseline	Our methodology
	STPA methodology	FMEA methodology	STPA-SysML methodology
analyzed object Sources of hazardous events Number of hazardous incidents Generating Scenes	control structure Based on expert knowledge 80 unsupported	Component Failure Modes Based on potential defects 54 unsupported	Security Analysis Model GUI based database 96 Support for automated scenario generation

VI. CONCLUSION

This paper identifies the vehicle-level potential hazard events of this self-driving car based on the traditional STPA method, and identifies the potential hazards of the vehicle by identifying the unsafe control behaviors of the system, and the results are compared as shown in Table XI.

The traditional STPA approach differs from the one proposed in this paper in the following four main ways:

(1) Analysis object: Most of the STPA methods identify system hazards from the control structure, and if the hazards at the software level are identified, it is necessary to abstract and reconstruct the software structure to a certain extent. The method proposed in this paper recognizes the system hazards from the finite state machine of the self-driving car, and the hazard events cover both software and hardware;

(2) The source of hazardous events: the STPA method is subjective and arbitrary in recognizing hazardous events. By applying the method proposed in this paper, the hazardous events are directly output from the finite state machine, which reduces the influence of subjective factors;

(3) Number of hazardous events: The unsafe control behaviors identified by the STPA method must be combined with the environmental conditions input by the experts to confirm whether or not they lead to a hazardous event. The method proposed in this paper determines the hazardous events directly by judging whether there is a conflict between the vehicle state and the environmental conditions;

Subsequent generation of scenarios: The STPA method has no way to generate scenarios directly. By applying the method proposed in this paper, the combination of the vehicle state and certain environmental conditions satisfies the definition of functional scenarios, so that test scenarios can be generated to verify the validity of the hazardous events.

we conduct a research on the expected functional safety hazard event identification method for automated driving systems. To address the deficiency that hazard event analysis does not cover the impact of the operating environment, we propose a new expected functional safety edge scenario identification method and develop software incorporating SysML elements, which demonstrates a significant improvement in the number of identifications and generalizability by comparing it with the expected functional safety hazard identification methods based on traditional methods such as STPA and FMEA. The experimental results show that our method is able to identify 20% more scenarios than the STPA method under experiments with automated lane keeping systems, i.e., from 80 scenarios to 96 scenarios accurately under the same test conditions. This advantage stems from the innovative introduction of graphical process metrics in our system modeling and analysis approach, as well as a more refined algorithm design. Compared to traditional methods, our approach is able to capture system-specific functions and potential failure modes more comprehensively, thus improving the recognition of edge scenes. In addition, in the future research, the following aspects will be centered on.

(1) Algorithm optimization: Further optimize the edge scene recognition algorithm in this paper to improve recognition accuracy and efficiency;

(2) Experimental extensions: Expanding the scale and diversity of experiments to validate the generalization and robustness of the methodology across different systems and scenarios;

(3) Practical application: Apply our methodology to real engineering projects to assess its practicality and feasibility in real system development.

Through continued in-depth research and continuous optimization, we believe that our methodology is expected to make an even more important contribution to the further development of the field of anticipatory functional safety, improving the safety and reliability of systems

VII. References

[1] DRESNER K, STONE P. A multiagent approach to autonomous intersection management [J]. Journal of artificial intelligence research, 2 [1]International Organization for Standardization. ISO 26262 Road vehicles-Functional safety [S]. Gereva, Switzerland: ISO, 2011 .

[2] International Organization for Standardization. ISO/PAS 21448: 2019 Road vehicles-Safety of the intended functionality [S]. Geneva, Switzerland : ISO, 2019 .

[3] ISO FDIS 21448, Road vehicles - Safety of the intended functionality [S].2021

[4] Walker A . SOTIF the Human Factor[C]. Communications in Computer and Information Science, vol 1060. 575-584, Springer, Cham.

[5] J. C. F. de Winter and D. Dodou, "Preparing drivers for dangerous situations: a critical reflection on continuous shared control," 2011 IEEE International Conference on Systems, Man, and Cybernetics, 2011, pp. 1050-1056.

[6] Happee Z, Cabrall R, Kyriakidis C, et al. Human factors of transitions in automated driving: a general framework and literature survey[J]. Transportation research, 2016, 43F(nov.):183-198.

[7] Ekereuke, Udoh, Vladimir, et al. Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving System[C]// 0.

[8] Li, J., Liu, L., & Gu, L. (2021). Understanding Take-Over in Automated Driving: a Human Error Analysis. HCI.

[9] Bainbridge, Lisanne. "Ironies of automation." Autom. 19 (1983): 775-779.

[10] Bibby, K. S., Fred Margulies, John E. Rijnsdorp, R. M. J. Withers and I. M. Makarov. "Man's Role in Control Systems." IFAC Proceedings Volumes 8 (1975): 664-683.

[11] Endsley, M. R., & Kiris, E. O. (1995). The Out-of-the-Loop Performance Problem and Level of Control in Automation. Human Factors, 37(2), 381-394.

[12] Hancock, P. A., Jagacinski, R. J., Parasuraman, R., Wickens, C. D., Wilson, G. F., & Kaber, D. B. (2013). Human-Automation Interaction Research: past, present, and future. Ergonomics in Design, 21(2), 9-14.

[13] Winter, Joost de, Riender Happee, Marieke H. Martens and Neville A. Stanton. "Effects of adaptive cruise control and highly automated driving on workload and situation awareness: a review of the empirical evidence." Transportation Research Part F-traffic Psychology and Behaviour 27 (2014): 196-217.

[14] Seppelt, Bobbie D. and Trent Victor. "Potential Solutions to Human Factors Challenges in Road Vehicle Automation." (2016).

[15] Kyriakidis, Miltos, Riender Happee and Joost de Winter. "Public opinion on automated driving: results of an international questionnaire among 5000 respondents." Transportation Research Part F-traffic Psychology and Behaviour 32 (2015): 127-140.

[16] QIU Y,MISU T,BUSSO C. Driving anomaly detection with conditional genera tive adversarial network using physiological and can bus data[C]//2019 International Conference on Multimodal Interaction,2019:164 173.

[17] Xu, Zhigang, Kaifan Zhang, Haigen Min, Zhen Wang, Xiangmo Zhao and Peng Liu. "What drives people to accept automated vehicles? Findings from a field experiment." Transportation Research Part C: Emerging Technologies (2018): n. pag.

[18] Blanco, Myra, Jon Atwood, Holland Marie Vasquez, Tammy E. Trimble, Vikki L. Fitchett, Joshua Radlbeck, Greg Fitch, Sheldon Russell, Charles A. Green, Brian Douglas Cullinane and Justin F. Morgan. "Human factors evaluation of Level 2 and Level 3 automated driving concepts." (2015).

[19] Zhang Yun, Li Ru, Jiao Weiyun, et al . Research on standardization of automatic driving function safety [J]. China Standardization, 2020(11): 109. zhang Yun , LI Ru , JIAO Weiyun , et al. Research on standardization of functional safety of automated driving system ［J］. Research on standardization of functional safety of automated driving system ［J］.

[20] Neubauer, Catherine, Gerald Matthews and Dyani Saxby. "The Effects of Cell Phone Use and Automation on Driver Performance and Subjective State in Simulated Driving." Proceedings of the Human Factors and Ergonomics Society Annual Meeting 56 (2012): 1987 - 1991.

[21] Piccinini, Rodrigues, Leitao. Reaction to a critical situation during driving with adaptive cruise control for users and non-users of the system[J]. Safety Science, 2015,72:116-126.