Manuscript Submitted to *Security and Safety,* For Peer Review Only, Vol. X, XXXXXXX (2023)
https://doi.org/10.1051/sands/XXXXXXX
sands.edpsciences.org

Automotive Industry

OPEN ACCESS

Section Category (Information Network/Integrated Circuits/Software Engineering/Industrial Control/Intelligent Transportation/Medical and Healthcare/Digital Finance/Social Governance/Other Fields)

Research on Functional Safety Design for Passenger Vehicles Based on STPA at the Vehicle Level

Yilin Zhong, Jinxiang Fang, Xiangjian Wang, Qingming Liu, Yuanhao Meng, Xiaoping Chen

BYD Auto Industry Co., Ltd., 518118 Shenzhen, China

Received: xx xxxxxxxx 2021 / Revised: xx xxxxx 2022 /Accepted: xx xxxxxxxxx 2022 / Published online: xx xxxxx 2023

Abstract Amidst the intelligent revolution reshaping the transportation industry, safety remains the top priority in vehicle manufacturing. International standards ISO 26262 (Road vehicles — Functional safety), ISO 21448 (Road vehicles — Safety of the intended functionality), and national standard GB/T 34590 (Road vehicles — Functional safety) define functional safety design and development processes for individual electronic/electrical systems. However, From an industry-wide perspective, the practice of treating passenger vehicles as complex integrated systems for functional safety analysis remains relatively limited. In particular, the collaborative application of ISO 26262 and SOTIF is still in the exploratory and refining stage. To a certain extent, this situation not only escalates the difficulty of identifying cross-system risks but also poses challenges to the development of a vehicle-level functional safety protection framework. This study focuses on the application of System-Theoretic Process Analysis (STPA) in vehicle-level functional safety analysis. By mapping its application pathways, we define a safety analysis methodology that integrates STPA with Hazard Analysis and Risk Assessment (HARA), enabling a shift from traditional single-system safety analysis to a system-engineering-aligned vehicle-level safety analysis. The proposed methodology effectively identifies vehicle-level functional safety risks, addressing a critical gap in industry practices. This research provides theoretical support and practical pathways for safety design in the era of intelligent vehicles.

Keywords Functional Safety of Passenger Vehicle; System-Theoretic Process Analysis, STPA; Hazard Analysis and Risk Assessment, HARA

Citation Yilin Zhong, Jinxiang Fang, Xiangjian Wang, Qingming Liu, Yuanhao Meng, Xiaoping Chen,. Research on Functional Safety Design for Passenger Vehicles Based on STPA at the Vehicle Level. Security and Safety 20XX; x: xxxxxxx. https://doi.org/10.1051/sands/xxxxxxx

1 Introduction

With the rapid development of the automotive industry, intelligent vehicles have become the mainstream direction of future automotive advancement. Compared to traditional vehicles, intelligent vehicles are reshaping the mobility experience through electrification, intelligence, and connectivity. However, technological architecture innovations and expanded application scenarios have introduced dual safety challenges for passenger vehicles. On one hand, ISO 21448 (Road vehicles — Safety of the intended functionality) requires systems to continuously maintain safe behavior in dynamic environments; on the other hand, cybersecurity threats—such as sensor data tampering—may penetrate into the physical control layer through software vulnerabilities. For example, a certain intelligent driving system once experienced erroneous path planning due to malicious interference with LiDAR point cloud data. Such incidents highlight the fragmentation between traditional functional safety analysis and cybersecurity protection. Furthermore, while the ISO 26262 (Road vehicles — Functional safety) standard focuses on hardware and software failure risks, ISO 21448 (SOTIF) emphasizes lifecycle-wide monitoring of system behavior, necessitating a more flexible analytical framework to enable their effective integration.

* Corresponding author (email: XXXXX@XXXXX)

Under this context, traditional component-failure-based safety analysis methods—such as Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) —are increasingly inadequate in addressing the complex interaction risks present in highly integrated systems. FMEA is a typical inductive analysis method. It enables an in-depth investigation into the failure effects of individual components within a system; however, it lacks effective countermeasures for analyzing system anomalies caused by coupling effects, common-cause failures, and interaction conflicts. FTA is a representative deductive analysis method, whose strength lies in logically deducing basic events from known top events and supporting the analysis of combined failures. Nevertheless, it is inadequate in identifying unknown system failure risks and addressing system anomalies induced by environmental factors and temporal conflicts. Hazard and Operability Study (HAZOP) is an emerging exploratory analysis method that analyzes the causes and consequences of process deviations from normal operating conditions, featuring structured cause investigation and consequence assessment. Yet it lacks effective solutions in aspects such as root cause localization and transient process condition analysis. Furthermore, all three aforementioned methods are deficient in the analysis and evaluation of dimensions including human-machine interaction effects and system-environment interaction effects, which are precisely key areas requiring focused analysis in the future development trend of automotive engineering. For instance, in the context of autonomous driving and electronically controlled steering, the emergence of system-level failure scenarios has imposed higher requirements on safety analysis techniques. System-Theoretic Process Analysis (STPA) breaks through the reductionist analytical paradigm. It constructs a closed-loop model based on control and feedback. Taking anomalies in the controlled process as the analytical entry point, this model can not only cover failures identified by traditional analysis methods, but also further capture analytical dimensions beyond the reach of conventional approaches by establishing human-machine control models, interaction models between control systems and the environment, and other relevant models. Owing to its unique accident causality model and system-level perspective, STPA has gradually become a core tool for addressing complex functional safety challenges.

This paper focuses on the application research of STPA in vehicle-level functional safety analysis for passenger cars. By mapping the application pathway of STPA in this context, it establishes a safety analysis methodology integrating STPA and Hazard Analysis and Risk Assessment (HARA). The methodology takes the passenger vehicle as a whole system, performs functional control domain partitioning according to vehicle motion control, energy control, and other aspects, constructs an analytical framework of "control actions – process states – safety constraints," and ultimately derives safety requirements oriented toward the vehicle-level.

2 Safety Analysis Methods

2.1 Deductive and Inductive Methods

The deductive method starts from general principles or hypothesized system-level failures and uses logical reasoning to identify specific components or system behaviors that could lead to such failures. Its advantage lies in narrowing the scope of analysis; however, it has inherent limitations. In contrast, the inductive method is based on observed or assumed specific states of system components—such as failure modes—and analyzes how these conditions affect the overall system safety. Nevertheless, the practical application of inductive methods is often constrained, as it is difficult to comprehensively identify all potential component failure modes or hazardous operating conditions [1].

To better understand the causes of accidents, event chain models are widely used. These models describe accident causation as a sequence of discrete events arranged in chronological order [2]. Among them, the Domino Model (Heinrich [3]) and the Swiss Cheese Model (Reason [4]) are typical representatives. Currently, FTA and FMEA are the most commonly used event chain analysis tools in practice.

FTA belongs to the "deductive" method, which determines how a given system state occurs and is therefore a "top-down" analytical approach [1], as shown in Figure 1. The analysis extends from the top event of the fault tree down to its leaf events, identifying combinations of failures that lead to the top event within the system context [5]. Failures can be events related to component malfunctions, human errors, or other contributing factors.

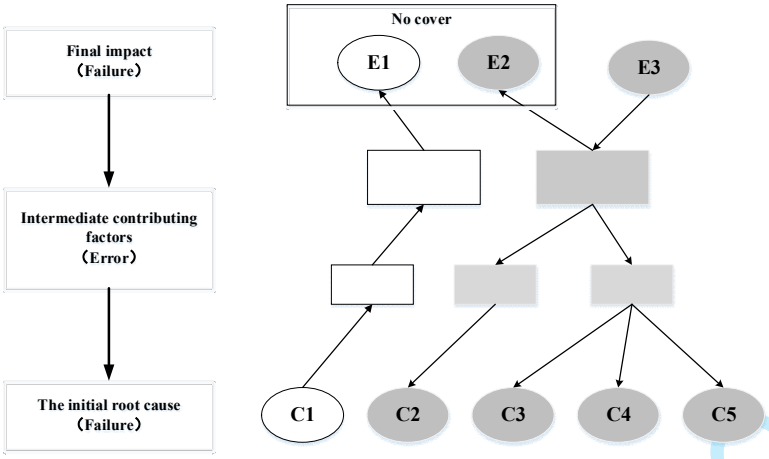

Figure 1. Top-down FTA method

FMEA is an "inductive" method, which identifies possible system states through a "bottom-up" analytical approach [1], as shown in Figure 2. FMEA begins with a system analysis, followed by listing as many potential failure modes of the target component as possible. It then analyzes the causes, effects, and existing control measures associated with each failure mode. Finally, it evaluates each mode based on severity (S), occurrence (O), and detectability (D), calculates the Risk Priority Number (RPN) accordingly [6].

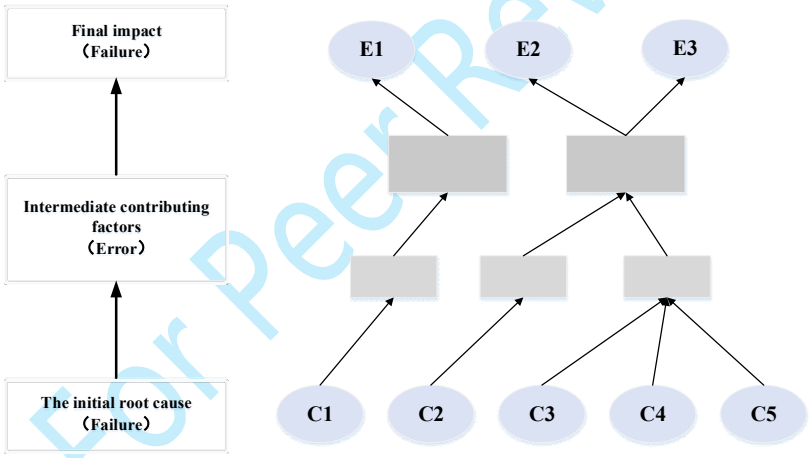

Figure 2. bottom-up FMEA method

In addition to FMEA, other inductive methods in the safety analysis domain include Failure Modes, Effects, and Diagnostic Analysis (FMEDA) and Event Tree Analysis (ETA).

HAZOP is a Process Hazard Analysis (PHA) method that lies between inductive and deductive approaches [7]. It uses guide words to systematically identify deviations from the intended design of the system or its components, assumes the presence of undesirable system behaviors, and identifies the hazards these deviations may cause [8]. Subsequently, brainstorming is conducted on the causes of each deviation within defined nodes, and the sequence of events leading to each cause is determined [9].

2.2 STPA

STPA is an advanced safety analysis technique proposed by Professor Nancy Leveson of the Massachusetts Institute of Technology [10-11]. Its theoretical foundation stems from the System-Theoretic Accident Model and Processes (STAMP) framework. STPA overcomes the limitations of linear causal chain models and takes a holistic system-level perspective, emphasizing the impact of systemic factors—such as unsafe interactions between components, software design flaws, and human decision-making errors—on safety

in complex system environments. STPA conducts safety analysis and safety design through four steps [12], as shown in Figure 3.

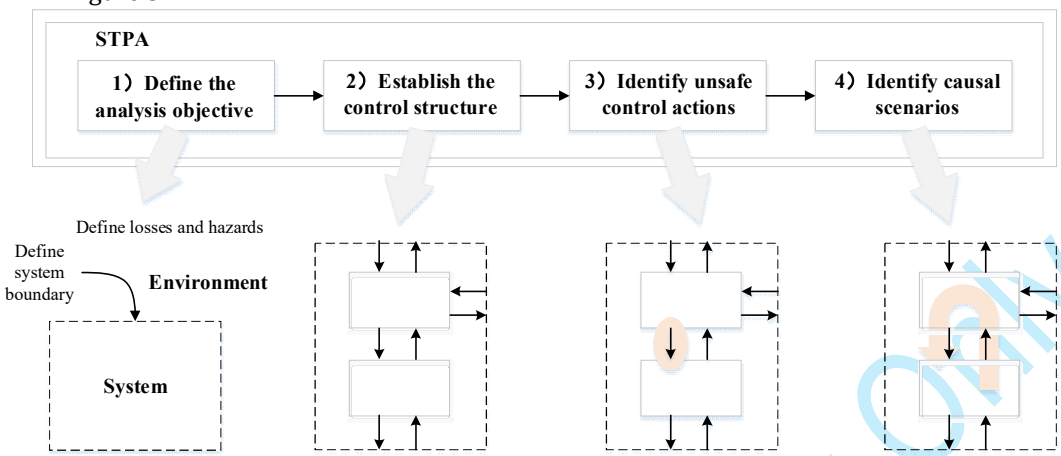

Figure 3. STPA steps

Step 1: Define the analysis objective – Establish the system boundary, define types of losses (e.g., casualties, equipment damage), system-level hazards (e.g., failure to maintain a safe distance between vehicles), and safety constraints (e.g., mandatory maintenance of a minimum safe distance).
Step 2: Develop the control structure – Construct a system control model that includes controllers, actuators, sensors, and feedback loops, clearly defining the interactions among components. For example, in an Autonomous Emergency Braking (AEB) system, the collaborative functions of the control module (ECU), ranging module, and braking module must be modeled.
Step 3: Identify Unsafe Control Actions (UCAs) – Analyze UCAs from four dimensions:1.Failure to provide a required control action, leading to hazard;2.Providing a control action that directly causes a hazard;3.Providing a potentially safe control action at the wrong time (too early, too late) or in the wrong sequence;4.Continuing a control action for too long or terminating it too early. For instance, in an AEB system, UCAs may manifest as "failing to trigger braking within the safe distance" or "prematurely triggering braking, causing vehicle instability."
Step 4: Identify causal scenarios – Investigate the underlying causes that may lead to UCAs, such as sensor data errors, algorithmic logic flaws, feedback delays, or human operator errors, and propose mitigation measures (e.g., enhancing algorithm redundancy or improving human-machine interface design).

2.3 Comparison of STPA with Traditional Safety Analysis Methods

When conducting safety analysis using event chain models such as FTA and FMEA, analysts typically treat accidents as a chain of sequential events. The FTA method starts from a top-level failure event (the top event) and works downward layer by layer to identify all logical combinations that could lead to the failure. However, for highly complex and tightly coupled systems—such as autonomous driving systems—this approach often fails to comprehensively capture all possible failure pathways. The FMEA method, on the other hand, primarily focuses on failure modes of individual components and their effects, emphasizing component reliability. Nevertheless, it is less effective in analyzing failures triggered by a common cause or multiple simultaneous failures [13].
When applying HAZOP for safety assessment, different combinations of guide words and parameters may sometimes produce the same deviation, leading to reduced study efficiency [14]. Moreover, while HAZOP uses a deductive approach to explore causes, it cannot accurately identify all possible combinations of causes that lead to a deviation. Due to these limitations, HAZOP is only suitable for analyzing relatively simple functional systems [13].
In contrast, the advantage of STPA lies in its ability to deeply investigate causal factors behind identified hazards. Compared to traditional hazard analysis methods, STPA considers a broader range of hazard causes, making it more applicable to safety analysis in complex systems [15].
Koelln [16] applied STPA, FTA, and FMEA to the safety analysis of autonomous vehicles and found that

STPA can identify a large number of failure types and includes cross-system factors in the analysis. Furthermore, STPA can incorporate human error, which is not supported by FTA or FMEA. In addition, FTA and FMEA are generally applicable only in the mid-to-late stages of analysis, primarily used to verify whether an existing design is safe [17]. STPA, however, supports application in the early stages of system development and allows iterative use at any phase of the development process. Making modifications during the early stages is more cost-effective and efficient than performing system iterations in later phases.

In summary, Table 1 compares the effectiveness of STPA, FTA, FMEA, and HAZOP in conducting safety analysis for autonomous driving systems.

Table 1. Comparison of different safety analysis methods

Evaluation dimensions	FTA	FMEA	HAZOP	STPA
Focus on interactions between systems	No	No	No	Yes
Focus on interactions between components	Poor	Poor	Medium	Excellent
Focus on component reliability	Medium	Excellent	Medium	Medium
Focus on cyber attacks	No	No	No	Yes
Focus on human-machine interaction	Poor	Poor	Medium	Capable
Applicable development phase	Mid to late stage	Mid to late stage	Early design	Early design
Abstract / Concrete	Concrete	Concrete	Abstract	Abstract
Complexity	Low	Low	High	High

2.4 Application Domains of STPA

STPA is widely applied across various industries, including military, maritime, healthcare, aerospace, nuclear power, transportation, and chemical industries.

Park [18] adopted the STPA method, focusing on the interactions among Maritime Autonomous Surface Ships (MASS), Remote Operation Centers (ROC), and Remote Operators (RO). Wong [19] pointed out that one challenge hindering the popularization of STPA is the difficulty in modeling and analyzing systems by constructing control structures. He proposed a method that leverages existing flowcharts when creating control structures. Koivisto [20] Koivisto [19] investigated the application of STPA within the context of probabilistic risk assessment. Using a case study on the standby cooling system of the refuelling pool in a nuclear power plant, the study demonstrated that STPA can identify all hazard scenarios previously detected by various techniques, including FMEA and Human Reliability Analysis (HRA). Suzuki [21] modeled the entire system as a hierarchical control structure and examined potential UCAs of each controller as well as their feedback paths. The analysis revealed hazard scenarios that may be overlooked by traditional failure-based methods. Larit [22] applied STPA to identify and mitigate hazards under free-flow conditions in MLC systems. The analysis highlighted UCAs, actuator delays, and sensor inaccuracies, and proposed recommendations for improving control logic, calibration, and response strategies to enhance system safety and reliability. To prevent near mid-air collisions or accidents during low-altitude UAV conflict resolution, Liu [23] transformed the safety issues in the process into control problems and proposed a safety analysis method for low-altitude UAV conflict resolution based on STAMP/STPA. Zhang [24] proposed an improved STPA method for risk analysis of hydrogen refueling stations. It aims to first define the objectives of risk analysis for the station system, and analyze the system-level losses, hazards, and constraints of the entire refueling station.

In recent years, an increasing number of scholars have begun introducing STPA into the field of connected and autonomous vehicles (CAVs), applying it to functional safety analysis of intelligent driving systems.

Chen [25] employed an STPA-guided approach to address the operational complexity of ADS in uncertain

environments, which involves the challenge of Safety of The Intended Functionality (SOTIF) assessment arising from potential combinations of multiple environmental factors and their continuous real-time behavior. Ejaz [26] demonstrated that STPA can effectively identify hazard causal factors in traffic systems involving autonomous vehicles; hazard causal factors within traffic systems are highly interconnected and coupled; and the Hazard Factor Network (HFN) provides a structured framework for the traceability and evaluation of causal factors. Özçetin O [27] conducted a SOTIF-based hazard analysis on the Adaptive Cruise Control (ACC) system using STPA. A total of 33 UCAs were identified, based on which vehicle-level safety constraints were defined. Zhao [28] applied STPA to analyze the adaptive cruise control system, specify its SOTIF requirements, and propose functional optimization targets for curved-road scenarios.

At the advanced application level, Soleimani [29] integrated STPA with the HARA process, enabling systematic classification of system-level performance-related hazards identified by STPA and the assignment of Automotive Safety Integrity Level (ASIL) through HARA. Chen [30] employed the STPA approach to guide the efficient exploration of the continuous state space of ADS hybrid automata under specific scenarios and identify hazardous conditions. Our method is implemented as SOTIFA, an automated end-to-end tool that integrates modeling, analysis, and risk assessment. Sun [31] introduced a fusion safety analysis method that provides a comprehensive assessment across these three domains. By identifying safety properties and mapping unsafe behaviors to hazardous scenarios, the method enables quantitative evaluation of integrated safety risks.

These studies demonstrate that the STPA method holds significant application value in safety analysis for intelligent and connected vehicles.

3 STPA Methodology for Vehicle Functional Safety

3.1 Establishment of the Five Major Functional Groups of the Complete Vehicle

The previous section introduced the theoretical foundation of this methodology based on STPA To enable functional safety design with the entire vehicle as the target, the vehicle's functions can be abstractly categorized along functional dimensions. Passenger vehicle functions can generally be divided into six major functional groups, as shown in Table 2.

Table 2. Function Group

Function Groups	Covered Functions
Motion Control (X-Axis)	Drive, Brake, Automatic Emergency Braking
Motion Control (Y-Axis)	Front-Wheel Steering, Rear-Wheel Steering, Lane Keeping Assist, Vehicle Stability Control
Motion Control (Z-Axis)	Intelligent Suspension Control
Energy Management Control	Battery Management, Charging Control, Power Control
Body Accessories Control	Doors, Windows, Wipers, Mirrors, Head-Up Display, Instrument Cluster Information, Infotainment Settings, etc.

3.2 Establishment of an STPA Methodology for Vehicle-Level Functional Safety

The standard steps of STPA have been elaborated in Chapter One. As shown in Figure 4, by introducing the evaluation metrics from HARA—namely severity, controllability, and exposure—the STPA methodology is enhanced to support the assessment of functional safety and SOTIF. This integration establishes a risk rating basis for identifying UCAs and effectively narrows the scope for subsequent causal analysis. This section will provide a detailed description of the STPA methodology tailored for vehicle-level functional safety.

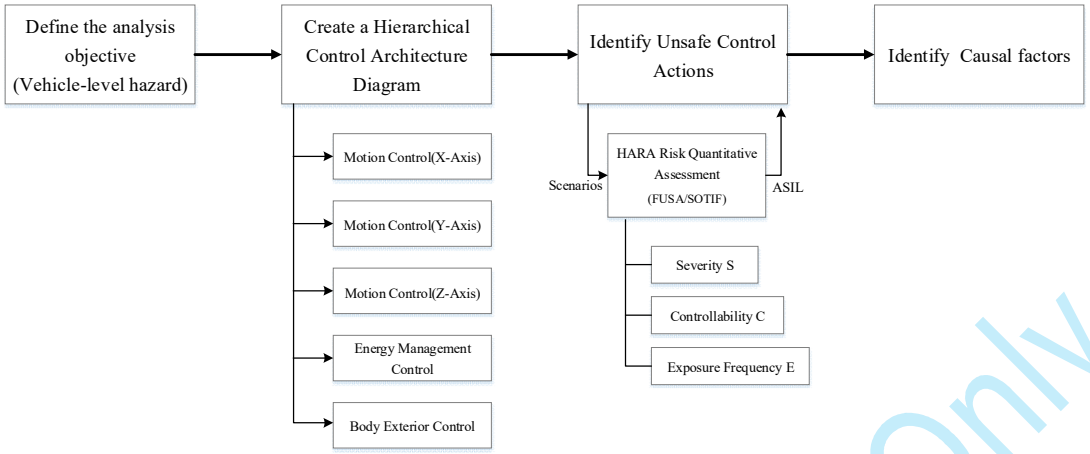

Figure 4. Vehicle-Level STPA Analysis Process

3.2.1 Define the analysis objective (Vehicle-level hazard)

In the standard STPA process, the first step is referred to as defining the analysis purpose. STPA requires users to typically define losses or accidents, identify system-level hazards, and establish system-level safety constraints in this initial step. This helps clarify the unacceptable hazard boundaries from stakeholders' perspectives, as well as the scope covered by the STPA safety analysis and design when applied to a specific system.

For complex systems, STPA begins its analysis by defining losses. Losses encompass not only injuries to people but also other types of losses (e.g., property damage, information leakage, reputational degradation). However, this paper discusses the STPA-based analytical approach strictly from a safety perspective. Therefore, the entry point of STPA analysis — defining losses — is directly focused on the analysis of human injury. Following the concept of functional safety, the potential sources of injury are defined as hazards. Hence, the primary focus of the first step in STPA is to define hazards, which are also referred to as vehicle-level hazards.

A vehicle-level hazard can be defined as an abnormality in vehicle-level functions (see Table 1) caused by the failure of a specific vehicle function, insufficient function definition, performance limitations, or reasonably foreseeable misuse by the driver — any of which may potentially serve as a source leading to human injury. Vehicle-level hazards are the result of propagated system-level hazards, where system-level hazards arise from failures of internal components within a system that implements a specific function, inadequate functional specification, or reasonably foreseeable human misuse causing abnormal function operation. Therefore, vehicle-level hazards can be avoided or controlled through functional safety and SOTIF activities.

Through the analysis of vehicle-level hazards, these hazards are categorized into motion-related hazards and non-motion-related hazards. Table 3 provide examples of vehicle-level hazards that align with the STPA framework. When conducting STPA safety analysis and functional safety design for the entire vehicle, engineers should typically, in the first step, comprehensively enumerate and summarize all potential hazards associated with the use cases of the analysis object, thereby establishing a hazard library.

Table 3. Vehicle-Level Hazards (Partial)

Category		Description
Motion-Related	Motion (X-Axis)	Unexpected acceleration
		Unexpected loss of acceleration
		Unexpected deceleration
		Unexpected loss of deceleration
		Reduction in vehicle deceleration
		Unexpected longitudinal movement

	Motion (Y-Axis)	Loss of longitudinal movement capability Longitudinal movement in the opposite direction to the intended direction Unexpected pitching motion ..... Unexpected lateral movement Loss of lateral movement capability Lateral movement in the opposite direction to the intended direction Unexpected yawing motion ..... Unexpected vertical movement
	Motion (Z-Axis)	Unexpected rolling motion .....
Non-motion-Related	Energy Management	Explosions caused by thermal release Explosions caused by gas discharge Thermal events Electrical shocks Generation of high temperatures or pressures Toxic gases causing direct harm to humans Loss or reduction of driver visibility .....
	Body Accessories	Driver receiving erroneous information Loss of warning Misjudgment by other drivers/pedestrians Loss of protection when vehicle safety systems are required to function .....

3.2.2 Create a Hierarchical Control Architecture Diagram

According to the STPA manual's definition, control structure modeling typically begins with abstracting the control structure and iteratively adding details. In many cases, the control structures and control loops within a system may be readily apparent or reusable from previous applications. This iterative approach of adding details also dictates that during the STPA process, the control structure undergoes continuous iteration based on the safety analysis workflow and results until it satisfies system-level constraints or safety requirements.

As mentioned in Section 3.1, to achieve functional safety design targeting the entire vehicle, the passenger car functions in this paper are divided into five major functional groups. The control architecture required by the STPA process will be derived in this paper's defined methodology by targeting each functional group.

Taking lateral motion control in passenger vehicles as an example, systems or functions within multiple functional safety boundaries typically contribute to overall lateral control. These include front-wheel steering, rear-wheel steering, lane-keeping assist, and electronic stability control. In traditional functional safety approaches, these systems or functions are often discussed as isolated entities, leading to potential oversights or omissions in their interactions. The methodology presented herein establishes all functions or systems involved in vehicle lateral motion control within a single control interface. Their interactions and information exchange are abstracted into the control actions and feedback signals required by the STPA control structure. This approach constructs a complete control flow diagram for achieving vehicle lateral motion control, ensuring functional safety compliance and integrity.

3.2.3 Identify UCAs

In the STPA handbook, the author identifies UCAs by examining each control action within the control structure, guided by the lead-in words and contextual cues. The lead-in words provided by STPA encompass the four categories mentioned in Table 4.

Table 4. UCA Guide Words (from the STPA handbook)

Guide Words	Definition
Needed but not provided	Control signals are sent to the actuator when unnecessary in this scenario, resulting in the hazards defined in Step 1 of the STPA.
Unneeded but provided	Control actions were not issued to the actuator when required by the scenario, resulting in the hazard defined in Step 1 of the STPA.
Provided at the wrong time	The timing of control signals sent to the actuator is either too early or too late, causing the hazards defined in Step 1 of the STPA to occur.
Duration error	Control signals sent to the actuator are either too long or too short in duration, causing the hazards defined in STPA Step 1 to occur.

Since the safety analysis defined in this paper is directly oriented toward functional safety, potential failure modes are typically derived by guiding functional aspects through prompting in the traditional HAZOP process. To ensure functional safety compliance and completeness, the prompts provided during HAZOP are also applied in this step. Specifically, the expanded prompts and their interpretations developed during the STPA process are presented in Table 5.

Table 5. UCA Guide Words (functional safety extension)

Guide Words	Definition
Provide strength error	Control actions sending excessive or insufficient force to the actuator may cause the hazards defined in STPA Step 1.
Provided but failed to execute	Control actions are issued to the actuator as required by the scenario, but the direction of the control action is erroneous or not correctly executed by the actuator, resulting in the hazard defined in STPA Step 1.

Additionally, the STPA process does not provide analysts with methods for quantifying ratings of hazards or hazardous events. To further ensure functional safety compliance and meet ISO 26262 requirements, this methodology also integrates the HARA process within Step 3 of STPA. It targets UCAs to perform ASIL-quantified assessments of the hazards and hazardous events they may cause under specific scenarios. This ensures that all safety analysis entries in subsequent STPA steps carry ASIL information.

3.2.4 Identify Causal factors

On the basis of the above analysis of UCA, it is necessary to further analyze the root causes leading to such UCAs, so as to formulate clear safety requirements for them. Through the transmission of requirements and requirement-based design, losses caused by unsafe control behaviors of the system during operation can be avoided, which constitutes the ultimate purpose of implementing STPA.

The causal analysis in STPA centers on UCAs, which are derived from the analysis of control actions. Therefore, the foundation of causal analysis lies in control actions. STPA establishes a closed-loop control-feedback model for control actions. This model consists of four basic elements: the controller (including human operators in human-machine analysis, who are regarded as possessing a mental model within the closed-loop control framework), the actuator, the sensor, and the controlled process. The information transmission media among these four elements (e.g., bus communication, energy transfer, etc.) are treated as another four fundamental elements. In addition, two supplementary elements are considered: the influence exerted by other controllers on the controlled process to cover analytical dimensions such as control conflicts, and the external inputs required for the execution of the controlled process. Altogether, these ten components constitute the basic elements of the closed-loop control model.

Based on the ten elements of the closed-loop control model, the unique failure modes of each element may lead to defined losses. These losses include not only electrical and electronic failures of concern in functional safety, but also performance limitations and human misuse addressed in the SOTIF, information intrusions emphasized in cyberattack, as well as non-electrical and non-electronic failures such as mechanical, chemical, and environmental failures. As illustrated in Figure 5 below, the causal analysis model is constructed by the closed-loop system composed of the above ten elements and the failure modes specific to each element.

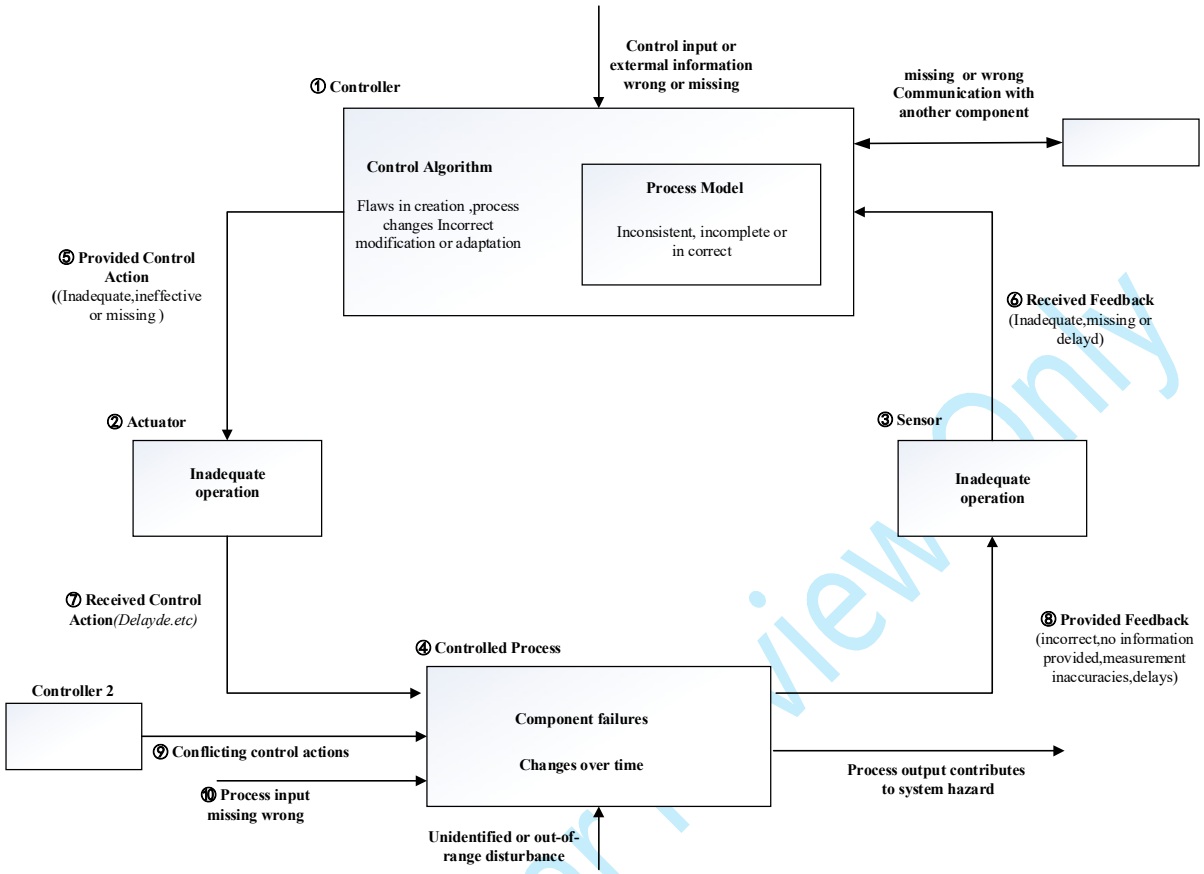

Figure 5. General Causal Analysis Model

The above causal analysis model serves as the general framework for causal analysis activities, but cannot fully cover all causal categories and refined causal factors. Therefore, this paper proposes a more comprehensive classification of causal types and detailed causal factors based on this model, as summarized in Table 6 below.

Table 6. Causal Factor Guide Words (Partial)

Causal Module	Causal Guideline Term	Example of Causal Factor
①②③ Failures Related to Controller/Sensor/Actuator	Inadequate Operation, Time-Dependent Failure	Internal hardware failure; Time-dependent degradation; Incorrect data storage or retrieval; .....
	Software Errors	Insufficient control algorithm; Defects in software code generation; .....
	Incomplete or Incorrect Process Model or Calibration	Incomplete or incorrect calibration of sensors or actuators, including degradation characteristics; Incomplete or incorrect control process model, including degradation characteristics; .....
	Incorrect or Lost External Control Input	Timing-related input incorrect or lost;

	or Information	Malicious intruder; Damaged signal; .....
	Low-Voltage Power Supply Failure	Loss of low-voltage power supply Incorrect low-voltage power supply (too high, too low, interference) Incorrect reference voltage .....
	External Interference	EMI or ESD Vibration or shock effects Moisture, corrosion, or contamination .....
④ Failures Related to Controlled Process	Component failure in controlled process, time-dependent changes	Internal hardware failure; Time-dependent degradation; .....
	External Interference	Vibration or shock effects; Extreme external temperature or thermal cycling; .....
	Hazardous Interaction with Other Vehicle Components	Vibration or shock effects; Magnetic interference; Overheating caused by other components; .....
	Output of Controlled Process Triggers System Hazard	Output of controlled process triggers system hazard; .....
⑤⑥ Failures in Control Loop and Feedback Loop	Open Circuit, Short Circuit, Loss, Intermittent Faults	Open connection, short to ground, short to power, short to other harnesses; Excessive contact resistance in connector; Adjacent pins in connector shorted; .....
	Communication Bus Errors	Bus overload or bus error; Signal priority too low; Malicious intruder; .....
	Incorrect Connection	Incorrect harness connection; Incorrect pin assignment; .....
	External Interference	EMI or ESD; Manufacturing defects or assembly issues; .....
⑦ Actuator to Controlled Process	Incorrect or Inadequate Execution due to Hardware Fault	Incorrect or Inadequate Execution due to Hardware Fault; .....
	Execution Delay	Execution Delay; .....
	Incorrect Connection between Actuator and Controlled Process	Incorrect Connection between Actuator and Controlled Process; .....
⑧ Controlled Process to Sensor	Incorrect or Lost Sensor Measurement	Incorrect sensor calibration / positioning
	Sensor Measurement Delay	Sensor Measurement Delay; .....
	Imprecise Sensor Measurement	Imprecise Sensor Measurement;

		.....
⑨ Other Controllers Acting on Controlled Process	Conflicting Control Behavior	Conflicting Control Behavior;
		.....
	Inadequate Operation, Time-Dependent	Insufficient operation, time-dependent changes;
⑩ Provider of Process Input	Changes	.....
to Controlled Process	Electrical Noise (excluding EMI or	Electrical Noise;
	ESD)	.....

In safety analysis, the causal factors within each module should be thoroughly analyzed based on the above closed-loop control model, focusing on their contribution to UCAs, in order to evaluate the likelihood and severity of these causes ultimately leading to vehicle-level hazards. Furthermore, the causal factors listed in Table 6 cover a wide range of failure modes, including electrical and electronic failures, mechanical and thermal damage, chemical corrosion, and others. Therefore, the scope of STPA-based safety analysis is broader.

Figure 6 shows a comparison between the results of STPA and FMEA based on the statistics from Application Case 1. It can be seen from the analytical results that by introducing broader analytical dimensions and more diverse causal factors, STPA identifies more loss-causing causal factors. A comparison of the results from Case 1 shows that the number of causal factors identified by STPA is 167.7% of that identified by FMEA, representing an increase of 67.7%.

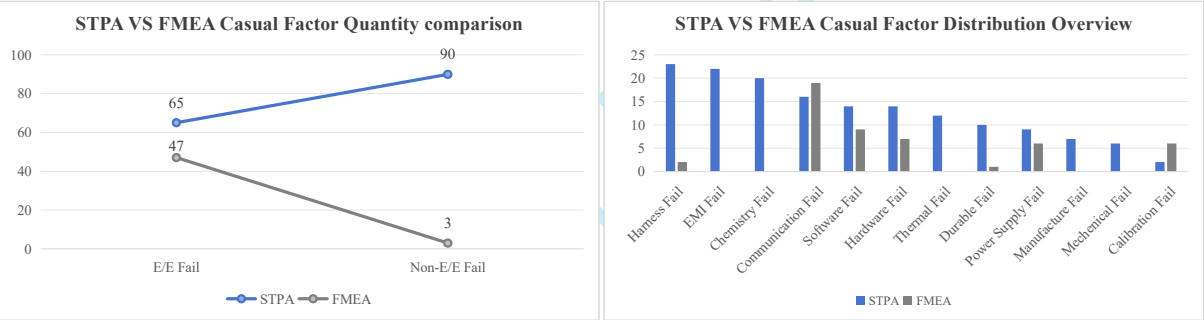

Figure 6. Comparison Between The Results Of STPA and FMEA

Figure 7 presents a comparison between the results of STPA and FTA based on statistics from Application Case 2.A comparison of the analytical results shows that the number of causal factors identified by STPA is 42.1% higher than that identified by FTA.

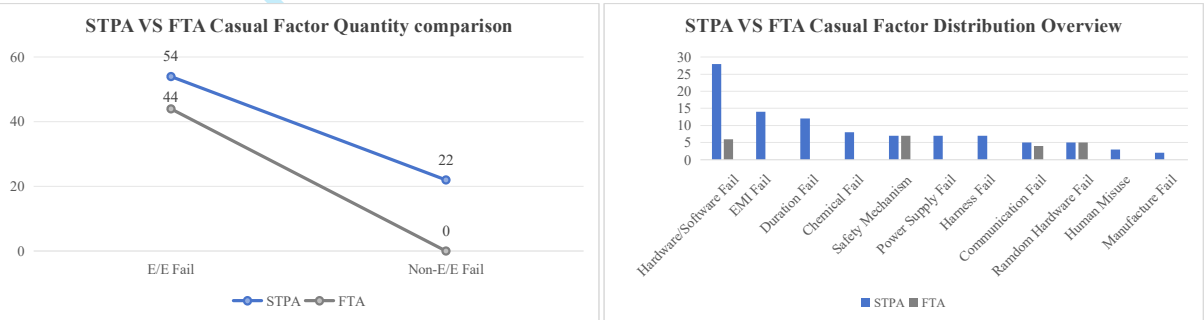

Figure 7. Comparison Between The Results Of STPA and FTA

4 Application Example

In this chapter, the Y-direction motion control of a passenger vehicle will be used as an example to conduct

a vehicle-level safety analysis based on the STPA methodology. Vehicle Y-direction motion control encompasses not only direct driver control but also indirect control by the intelligent driving system in autonomous driving mode, as well as human-machine cooperative driving. The causal analysis results obtained through STPA will be used to derive safety requirements.

4.1 Define the purpose of the analysis (Motion control(Y-Axis) vehicle-level hazards)

According to the method described in Section 3.2.1 for defining the analysis purpose in STPA, the primary focus in safety analysis is to define vehicle-level hazards. By describing and summarizing these vehicle-level hazards, the hazards associated with Y-direction motion control can be extracted from Table 3, as shown in Table 7.

Table 7. Vehicle-level hazard of Motion control(Y-Axis)

Category	Description
Motion control(Y-Axis)	[H1] Unintended Lateral Motion
	[H2] Loss of Lateral Motion Capability
	[H3] Lateral Motion in the Opposite Intended Direction
	[H4] Unintended Yaw Motion

4.2 Establish Hierarchical Control Architecture Diagram for Y-Direction Motion

The control structure serves as a prerequisite input for STPA safety analysis, providing a closed-loop control-based abstraction of Y-direction motion control from a vehicle-level perspective. It requires analyzing the underlying control logic that enables the vehicle to generate lateral motion. According to fundamental vehicle dynamics principles, there are two primary factors contributing to vehicle lateral (Y-direction) motion:

1) The steering system exerts lateral force on the tires, causing the wheels to rotate about the Z-axis (steering angle), thereby inducing lateral vehicle movement;
2) The braking system applies differential braking forces to individual wheels, creating speed differences among the four tires, which generates a yaw moment and consequently induces lateral motion.

Based on this foundational understanding of the underlying control logic for vehicle Y-direction motion, a hierarchical abstraction of the control logic can be systematically constructed, establishing a multi-layered control architecture.

Figure 8 below illustrates the logical control structure for vehicle-level Y-direction motion control derived from this analysis process.

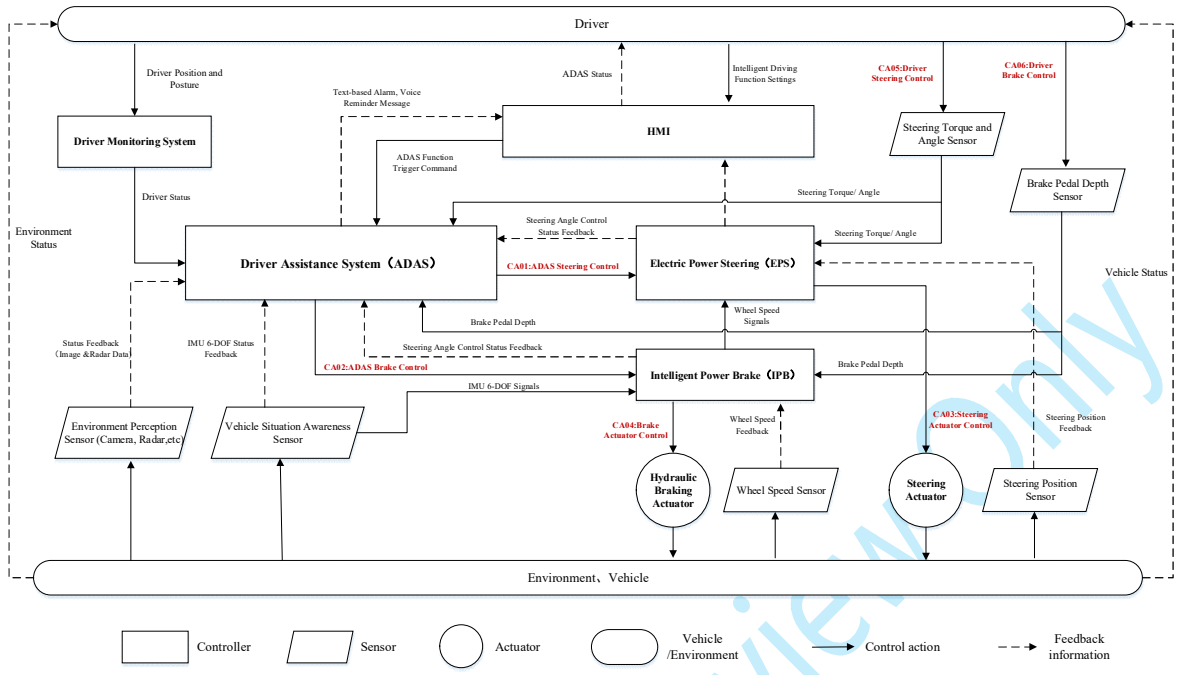

Figure 8. Hierarchical Control Architecture Diagram for Y-Direction Motion

In Figure 8,At the topmost layer is the driver (assuming no higher-level coordination center exists). The next layer includes the driver's control actions applied to the vehicle and bidirectional information exchange, such as steering input and braking input. Information interaction includes HMI warning messages and driver status information (e.g., attention level, posture);The subsequent layer is the vehicle controller layer, including the intelligent driving system controller, brake controller, and steering controller. The intelligent driving controller sends high-level braking or steering commands to the brake or steering controllers, forming a refined control sub-layer.Below this is the actuator and sensor layer, including brake actuators and steering actuators, along with corresponding feedback sensors—wheel speed sensors and steering angle sensors—that form closed-loop control. Additionally, environmental perception sensors (e.g., camera, radar) and vehicle state perception sensors (e.g., IMU, yaw rate sensor) are included for intelligent driving closed-loop control;At the bottom is the controlled process layer and environmental layer, representing the physical vehicle dynamics and external driving environment.It should also be noted that the driver, acting as the top-level "controller," directly perceives environmental conditions and vehicle dynamic states through human sensory organs (vision, hearing, vestibular sense), forming a natural feedback loop for closed-loop control.This control structure exemplifies a typical STPA control architecture and holds significant engineering reference value.

We derived vehicle lateral (Y-direction) motion control actions based on Figure 8. resulting in 6 key control actions, as shown in Table 8.

Table 8. Control Actions

ID	Control Actions
CA01	ADAS Steering Control
CA02	ADAS Brake Control
CA03	Steering Actuator Control
CA04	Brake Actuator Control
CA05	Driver Steering Control

CA06	Driver Braking Control

4.3 Identify UCAs

In the standard STPA process, UCAs are a further analysis activity based on the premise of control actions. This analysis evaluates the sources of potential abnormal behaviors in control actions within the control system that could ultimately lead to vehicle-level hazards. These sources include not only control actions from internal vehicle systems but also external inputs—such as those from the driver—applied to the vehicle. Therefore, this analysis covers not only system-related functional insufficiencies or performance limitations (e.g., expected functional failures or underperformance), but also human misuse and other behavioral factors. Based on this concept, STPA supports both functional safety analysis and SOTIF, and further extends to non-electrical/electronic domains (as will be elaborated in the subsequent causal factor analysis), enabling a broader scope of safety analysis.

The process of analyzing control actions to identify UCAs primarily refers to the HAZOP-guided approach. Control actions are examined using the guide words listed in Table 4 and Table 5 to explore potential UCAs. By evaluating whether such deviations, when applied, would result in vehicle-level hazards based on actual vehicle behavior, it is determined whether a given control action under a specific guide word constitutes an UCA.

In the following analysis, CA01, CA03, and CA05 — representing intelligent driving steering control, steering actuator control, and human-driven steering control, respectively—will be used to conduct UCA analysis for Y-direction motion control. This analysis will ultimately support the identification of causal factors related to both functional safety and SOTIF, and enable the derivation of corresponding safety requirements, as shown in Table 9.

Table 9 UCAs analysis for CA01/CA03/CA05

	CA01:ADAS Steering Control	CA03:Steering Actuator Control	CA05:Driver Steering Control
GUI1: Required but Not Provided	UCA0101: When the vehicle requires steering under intelligent driving mode, the intelligent driving system controller fails to issue the [CA01] control action to the steering actuation system, resulting in hazard [H2] — Loss of Lateral Motion Capability.	UCA0301: When the steering controller receives a steering control request from either the intelligent driving system or the driver, it fails to issue the [CA03] control action to the steering actuator, resulting in hazard [H2] — Loss of Lateral Motion Capability.	UCA0501: When the vehicle requires steering under human-driven mode, the driver fails to issue the [CA05] control action to the steering actuation system, resulting in hazard [H2] — Loss of Lateral Motion Capability.
GUI2: Not Required but Provided	UCA0102: When no steering is required under intelligent driving mode, the intelligent driving system controller issues the [CA01] control action to the steering actuation system, resulting in hazard [H1] — Unintended Lateral Motion.	UCA0302: When no steering command is received from the intelligent driving system or the driver, the steering controller issues the [CA03] control action to the steering actuator, resulting in hazard [H1] — Unintended Lateral Motion.	UCA0502: When no steering is required under human-driven mode, the driver issues the [CA05] control action to the steering actuation system, resulting in hazard [H1] — Unintended Lateral Motion.
GUI3: Incorrect Timing of Provision	Too Early: Same as UCA0102 Too Late: Same as UCA0101	Too Early: Same as UCA0302 Too Late: Same as UCA0301	Too Early: Same as UCA0502 Too Late: Same as UCA0501

GUI4: Incorrect Duration	Too Short: UCA0103: When steering is required under intelligent driving mode, the intelligent driving system controller issues the [CA01] control action to the steering actuation system, but the duration is too short, resulting in hazard [H2] — Loss of Lateral Motion Capability.	Too Short: UCA0303: When the steering controller receives a steering control request from the intelligent driving system or the driver, it issues the [CA03] control action to the steering actuator, but the duration is too short, resulting in hazard [H2] — Loss of Lateral Motion Capability.	Too Short: UCA0503: When steering is required under human-driven mode, the driver issues the [CA05] control action to the steering actuation system, but the duration is too short, resulting in hazard [H2] — Loss of Lateral Motion Capability.
	Too Long: UCA0104: When steering is required under intelligent driving mode, the intelligent driving system controller issues the [CA01] control action to the steering actuation system, but the duration is too long, resulting in hazard [H1] — Unintended Lateral Motion.	Too Long: UCA0304: When the steering controller receives a steering control request, it issues the [CA03] control action to the steering actuator, but the duration is too long, resulting in hazard [H1] — Unintended Lateral Motion.	Too Long: UCA0504: When steering is required under human-driven mode, the driver issues the [CA05] control action to the steering actuation system, but the duration is too long, resulting in hazard [H1] — Unintended Lateral Motion.
GUI5: Incorrect Control Intensity	Too Low: UCA0105: When steering is required under intelligent driving mode, the intelligent driving system controller issues the [CA01] control action to the steering actuation system, but the control intensity is too low, resulting in hazard [H2] — Loss of Lateral Motion Capability.	Too Low: UCA0305: When the steering controller receives a steering control request, it issues the [CA03] control action to the steering actuator, but the control intensity is too low, resulting in hazard [H2] — Loss of Lateral Motion Capability.	Too Low: UCA0505: When steering is required under human-driven mode, the driver issues the [CA05] control action to the steering actuation system, but the control intensity is too low, resulting in hazard [H2] — Loss of Lateral Motion Capability.
	Too High UCA0106: When steering is required under intelligent driving mode, the intelligent driving system controller issues the [CA01] control action to the steering actuation system, but the control intensity is too high, resulting in hazard [H1] — Unintended Lateral Motion.	Too High: UCA0306: When the steering controller receives a steering control request, it issues the [CA03] control action to the steering actuator, but the control intensity is too high, resulting in hazard [H1] — Unintended Lateral Motion.	Too High: UCA0506: When steering is required under human-driven mode, the driver issues the [CA05] control action to the steering actuation system, but the control intensity is too high, resulting in hazard [H1] — Unintended Lateral Motion.
GUI6: Action Provided but Incorrectly Executed	UCA0107: When steering is required under intelligent driving mode, the intelligent driving system controller issues the [CA01] control action to the steering actuation system, but the actuation system executes the reverse action, resulting in hazard [H1] — Unintended Lateral Motion.	UCA0307: When the steering controller receives a steering control request, it issues the [CA03] control action to the steering actuator, but the actuator performs a feedback action instead, resulting in hazard [H1] — Unintended Lateral Motion.	UCA0507: When steering is required under human-driven mode, the driver issues the [CA05] control action to the steering actuation system, but the actuation system executes the reverse action, resulting in hazard [H1] — Unintended Lateral Motion.

Through the above analysis process, the derivation of UCAs in STPA has been completed. Different UCAs

lead to different vehicle-level hazards, and thus theoretically result in varying levels of severity. At the same time, it is also possible for different UCAs to lead to the same vehicle-level hazard, resulting in an identical level of severity. However, for vehicle-level hazards caused by a specific UCA, there remains a lack of assessment regarding the controllability (i.e., the possibility of avoiding the risk through driver or system intervention) and exposure (i.e., how frequently or under what conditions the scenario occurs). To address this gap, a risk level assessment is further established based on the STPA-derived UCAs to support the development activities of both functional safety and SOTIF.

Referring to the risk assessment model used in functional safety, scenarios are introduced on top of vehicle-level hazards to form hazard events. The hazard events are then scored in terms of severity, exposure, and controllability, enabling the derivation of the ASIL and determining whether SOTIF analysis is required. As shown in Tables 10, 11, and 12, risk assessment results are presented for three selected UCAs—UCA0101, UCA0302, and UCA0503—as examples, based on scenario modeling referenced from SAE J2980[33] .

Table 10. The HARA Process of UCA0101

UCA	Road Type	Road Condition	Environental Condition	Vehicle State	Relative Speed (km/h)	Special Elements	Hazard Event	Severity (S)	Exposure (E)	Controllability (C)	Functional Safety ASIL	SOTIF Required
UCA0101	Highway	Curve	Daytime	Forward Uniform Speed	(90, 120]	Cement barrier at roadside	Vehicle is on a curve under intelligent driving mode; the intelligent driving controller fails to issue a steering command, resulting in loss of lateral motion capability and ultimately leading to a rigid collision with the roadside barrier	3	4	1	B	Y
UCA0101	Urban Road	Curve	Nighttime	Forward Uniform Speed	(30, 60]	Pedestrians at roadside	Vehicle is on a curve under intelligent driving mode; the intelligent driving controller fails to issue a steering command, resulting in loss of lateral motion capability and ultimately leading to a collision with	3	4	2	C	Y

							pedestrians at the roadside					
...	...	...	...	...	...	...	...	...	...	...	...	...

Table 11. The HARA Process of UCA0302

UCA	Road Type	Road Condition	Environental Condition	Vehicle State	Relative Speed (km/h)	Special Elements	Hazard Event	Severity (S)	Exposure (E)	Controllability (C)	Functional Safety ASIL	SOTIF Required
UCA0302	Highway	Straight	Daytime	Forward Uniform Speed	(90, 120]	Oncoming vehicle in adjacent lane	Vehicle is on a straight road; the steering controller issues a steering command to the actuator without receiving any request from the intelligent driving system or driver, causing unintended lateral motion and ultimately resulting in a side collision with a vehicle in the adjacent lane	3	4	3	D	Y
UCA0302	Urban Branch Road	Straight	Daytime	Forward Uniform Speed	(30, 60]	Oncoming vehicle in adjacent lane	Vehicle is on an urban branch road; the steering controller issues a steering command without receiving any request, causing unintended lateral motion and ultimately	3	4	3	D	Y

							resulting in a head-on collision with a vehicle in the adjacent lane					
...	...	...	...	...	...	...	...	...	...	...	...	...

Table 12. The HARA Process of UCA0503

UCA	Road Type	Road Condition	Environental Condition	Vehicle State	Relative Speed (km/h)	Special Elements	Hazard Event	Severity (S)	Exposure (E)	Controllability (C)	Functional Safety ASIL	SOTIF Required
UCA0503	Rural Road	Curve	Nighttime	Forward Uniform Speed	(30, 60]	Steep slope beside the road	Under human-driven mode, the driver issues a steering command but the duration is too short, resulting in insufficient lateral motion, causing the vehicle to leave the road and fall down the slope	3	2	-	-	Y
UCA0503	Highway	Curve	Daytime	Forward Uniform Speed	(90, 120]	Intelligent driving mode activated, cement barrier at roadside	After switching from intelligent driving to human-driven mode, the driver issues a steering command but the duration is too short, resulting in insufficient lateral motion and a rigid collision with the roadside barrier	3	4	-	-	Y
...	...	...	...	...	...	...	...	...	...	...	...	...

The above risk assessment approach—combining vehicle-level hazards with operational scenarios—has yielded evaluation results for both functional safety and SOTIF. This provides methodological support

based on STPA for the concept development phase of functional safety and SOTIF. Table 13 below summarizes the results of the above risk assessments and serves as an analytical input premise for subsequent causal factor analysis.

Table 13. Summary of Risk Assessment for UCAs

UCA	Functional Safety Risk Assessment Result (ASIL)	SOTIF Assessment Result (Y/N)
UCA0101	C	Y
UCA0302	D	Y
UCA0503	-	Y

4.4 Identify causal factors

The prerequisite for identifying causal factors of an UCA is to fully consider all elements associated with the corresponding control action. By augmenting the basic closed-loop control model with these relevant factors, a comprehensive Causal Analysis Control Model—such as the one shown in Figure 5—is ultimately formed. Causal factors are then derived by applying the guiding words listed in Table 6 to this complete control model.

The Figure 9 shows the control model for CA01, which is formed by supplementing the original basic control model with additional information regarding the system architecture.

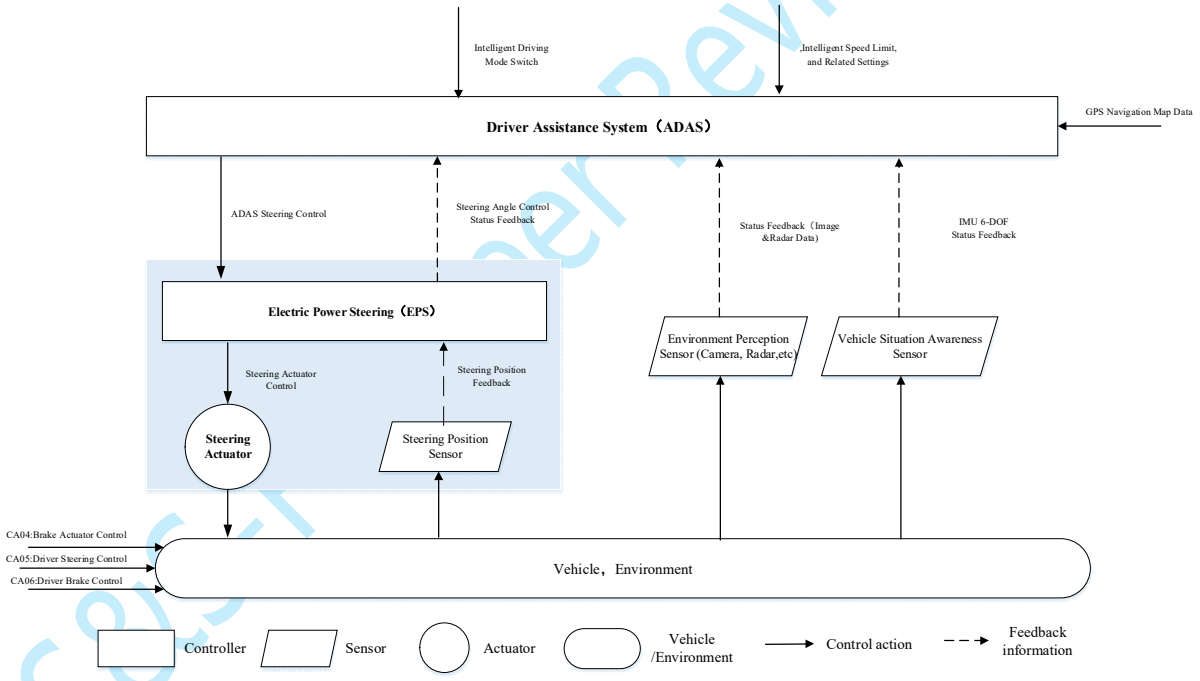

Figure 9. CA01 Causal Factor Analysis Model

Next, based on the guiding words in Table 6, the causal factors leading to the UCA can be identified. Corresponding safety requirements are then derived with respect to these causal factors and the desired safe state of the function. As shown in Table 14 below, an example of the causal factors and safety requirements (partial) for the instance UCA0101 is provided.

Table 14. Causal Factors and Functional Safety Requirements for UCA0101 (Partial)

Causal Module	Causal Guideword	Causal Factor	Safety Requirement	Causal Attribute
Intelligent Driving System Controller	Inadequate operation, time-dependent failure	Hardware failure within the intelligent driving system controller leads to the UCA0101	The intelligent driving controller shall perform hardware safety analysis to identify hardware failures causing UCA0101, and design safety mechanisms such as hardware fault monitoring and redundant switching to prevent the UCA0101	Functional Safety
	Incomplete or incorrect process model or calibration	Defects in the driving decision-making model of the intelligent driving system controller (due to insufficient environmental data training) lead to the UCA0101	The driving decision-making model of the intelligent driving system controller shall undergo sufficient training with environmental data, and corresponding scenarios shall be designed for closed-loop testing to reduce unknown scenarios to an acceptable level	SOTIF
	Incorrect or missing external control input or information	The intelligent driving system controller receives erroneous navigation data, leading to incorrect steering decisions and ultimately resulting in the UCA0101	The intelligent driving system shall receive navigation data from multiple sources through diverse channels and perform data validation via sensor/data fusion; if the validated data is found to be unreasonable, the system shall exit autonomous driving mode or degrade operation accordingly	SOTIF
	Incorrect or missing external control input or information	Ambiguous semantic feedback from the intelligent driving system to the driver causes the driver to inadvertently deactivate the system, leading to incorrect steering decisions by the intelligent driving system and ultimately resulting in the UCA0101	The intelligent driving system shall be designed with appropriate human-machine interaction (HMI) alert functions to prevent misuse of the intelligent driving system by the driver	SOTIF
	Low-voltage power supply failure	Loss of power supply to the intelligent driving system controller results in failure to issue correct steering control requests, leading to the UCA0101	The vehicle's low-voltage power supply system shall provide two redundant power supplies to the intelligent driving system controller, and the two redundant power paths shall meet independence requirements	Functional Safety
	.....	.....	.....	.....
Environmental Perception Sensor	Inadequate sensor operation, time-dependent degradation	Degradation of image sensor lens performance over time leads to inaccurate capture of road information, causing the intelligent driving controller to issue incorrect steering commands, resulting in the UCA0101	The image sensor shall undergo durability testing under real-vehicle environmental conditions, and performance acceptance criteria after aging shall be established to ensure that post-durability performance meets requirements	Functional Safety / SOTIF

	External Interference	Electromagnetic interference during radar sensor transmission and reception causes incorrect distance measurement, leading to the intelligent driving controller issuing incorrect steering commands and ultimately resulting in the UCA0101	The radar sensor shall undergo electromagnetic interference (EMI) assessment under real-vehicle environmental conditions; electromagnetic compatibility (EMC) acceptance criteria shall be defined, and EMC-oriented design and testing shall be implemented	Functional Safety / SOTIF
	Performance Limitation	The image sensor fails to correctly capture road image information due to strong backlighting or low road surface reflectivity, leading to the intelligent driving controller issuing incorrect steering commands and ultimately resulting in the UCA0101	The image sensor shall be evaluated for its performance limitations based on its working principles; mitigation measures shall be designed, and real-world test scenarios shall be developed for sufficient validation testing	SOTIF
	.....	.....	.....	.....
	Hardware open circuit, short circuit, loss, intermittent fault	The sensing signal line of the environmental perception sensor becomes disconnected due to loose connector, causing the intelligent driving controller to not receive valid environmental perception data, thereby issuing incorrect steering control commands and resulting in the UCA0101	The environmental perception sensor shall be designed with redundant sensing paths, and redundancy independence shall be maintained. The intelligent driving controller shall implement a validation mechanism to detect anomalies in perception signals, and the perception function shall integrate multi-sensor data fusion.	Functional Safety
Feedback Loop	Communication Bus Error	The data from the environmental perception sensor on the bus is maliciously tampered with by external network intrusion, causing the intelligent driving controller to receive incorrect perception data, thereby issuing incorrect steering commands and ultimately leading to the UCA0101	The intelligent driving controller shall implement cybersecurity design to prevent abnormal control caused by external network intrusion.	Functional Safety & Cybersecurity
	Controlled Process	Conflicting control actions	The braking control system triggers vehicle stability control (VSC), applying different braking forces to the four wheels, which causes vehicle yaw motion that conflicts with the front-wheel steering command from the intelligent driving controller, resulting in abnormal overall vehicle	The vehicle system shall evaluate abnormal steering behavior caused by the simultaneous

		steering and leading to the UCA0101	operation of braking-based vehicle stability control and intelligent driving steering control, and sufficient functional definitions shall be designed to avoid control conflicts.
.....	.....	.....	.....

5 Conclusion

This paper establishes a safety analysis methodology based on the integration of STPA and HARA, constructing an analytical framework of "control action – process state – safety constraint" to derive safety requirements at the vehicle level. Compared with traditional analysis methods, this approach offers the following specific advantages:

1. Supports safety analysis at the vehicle level. The STPA method is capable of analyzing systems with higher complexity. By establishing a hierarchical control feedback loop model for complex systems, it achieves a holistic abstract representation of the system's control structure. Based on this structure, control actions are extracted, and by taking control actions as the starting point of analysis, the method derives the relationship between safety requirements and vehicle-level hazards, thereby enabling a mapped linkage between safety requirements and the overall vehicle system.
2. Enables integrated analysis of functional safety and SOTIF. The STPA method can unify the previously separate analyses of functional safety and SOTIF into a single, comprehensive framework. During the analysis, it not only identifies hazards caused by conventional electrical/electronic failures but also recognizes hazards arising from non-electrical/electronic factors—such as performance limitations, environmental conditions, or unknown scenarios—as well as control conflicts between different systems at the vehicle level. These aspects are typically beyond the scope of traditional, single-dimension safety analyses.
3. Supports coordinated analysis of cybersecurity and functional safety. STPA allows the incorporation of cybersecurity-related guidewords into causal analysis, enabling collaborative assessment of cybersecurity and functional safety. This not only improves the coverage of safety analysis but also ensures consistency between the two domains, minimizing conflicts in safety requirements derived from separate analyses. It provides a foundational approach for broader safety integration.

Meanwhile, through analysis and practical experience, it is recognized that current applications of STPA still face challenges such as selecting appropriate levels of model abstraction and managing computational complexity. Future research should focus on three key areas: 1) developing automated modeling tools to reduce the cost of manual analysis; 2) exploring AI-driven dynamic scenario generation techniques to enhance the prediction of unknown risks; and 3) advancing the integration of STPA with digital twin technology to enable closed-loop iteration between virtual validation and real-world testing. With the widespread adoption of technologies such as 5G and V2X, STPA is expected to evolve further toward "real-time" and "collaborative" capabilities, providing sustained momentum for the safety advancement of intelligent vehicles.

In summary, STPA, as an innovative tool for system-level safety analysis, is driving the transformation of passenger vehicle functional safety from "component reliability" to "system behavior controllability." This

study, through theoretical development and case validation, provides a reference for the in-depth application of STPA in vehicle-level safety analysis, supporting the intelligent vehicle industry's pursuit of the "zero-risk" goal.

Acknowledgments

We would like to thank all editors and reviewers who helped us improve the paper.

Funding

This work was supported by BYD Company Limited.

Conflicts of interest

The authors declare no conflicts of interest.

Data availability statement

No data are associated with this article.

Author contribution statement

Yilin Zhong: Conceptualization, Methodology, Writing - Review & Editing, Supervision, Project administration; Jinxiang Fang: Methodology, Supervision, Writing - Review & Editing; Xiangjian Wang: Formal analysis, Data Curation, Literature review, Writing - Original Draft; Qingming Liu, Yuanhao Meng and Xiaoping Chen: Data Curation, Formal analysis, Proofreading and correcting typographical errors.

References

[1] U.S. Nuclear Regulatory Commission. Fault Tree Handbook[EB/OL].(1981-01)[2024-06-13].https://www.nrc.gov/docs/M-L1007/ML100780465.pdf.
[2] Wong L M, Pawlicki T. A review of accident models and incident analysis techniques[J]. Journal of Applied Clinical Medical Physics, 2025, 26(3): e14623.
[3] HEINRICH H.W.Industrial Accident Prevention: A Scientific Approach[M].New York: McGraw-Hill,1931.
[4] REASON J.Human Error[M].Cambridge:Cambridge University Press,1990.
[5] Stoelinga M, Ruijters E, Krčál P. Concise Guide to Fault Tree Analysis: Models, Methods and Algorithms[M]. Springer Nature, 2026.
[6] Cardiel-Ortega J J, Baeza-Serrato R. Probabilistic fuzzy system for evaluation and classification in failure mode and effect analysis[J]. Processes, 2024, 12(6): 1197.
[7] Mandali H, Keighobadi E, Ebrahimi H, et al. Machine learning and bayesian network based on fuzzy AHP framework for risk assessment in process units[J]. Scientific Reports, 2025, 15(1): 39083.
[8] Tian B, Li H, Cui X, et al. A HAZOP-based hazard identification model for urban gas accidents: Development and empirical validation[J]. Plos one, 2025, 20(10): e0333431.
[9] Salimi F F, Safavi A A, Urbas L, et al. A New Approach to HAZOP of Complex Chemical Processes[M]. Elsevier, 2023.
[10] LEVESON N G. A New Accident Model for Engineering Safer Systems[J]. Safety Science, 2004, 42(4):237-270.
[11] Falegnami A, Tomassi A, Corbelli G, et al. Managing complexity in socio-technical systems by mimicking emergent Simplicities in nature: a brief communication[J]. Biomimetics, 2024, 9(6): 322.
[12] Feng Y, Pan W, Wang R, et al. A Hybrid STPA-BN Framework for Quantitative Risk Assessment of Runway Incursions: A Case Study of the Austin–Bergstrom Incident[J]. Applied Sciences, 2026, 16(6): 2711.
[13] SUN L, LI Y F, ZIO E. Comparison of the HAZOP, FMEA,FRAM, and STPA Methods for the Hazard Analysis of Autom-atic Emergency Brake Systems[J]. ASME J. Risk Uncertainty Part B, 2022, 8(3): 031104.
[14] Chia M F, Narahariseti P K. HAZOP using Stateflow software: Methodology and case study[J]. Process Safety and Environmental Protection, 2023, 179: 137-156.
[15] Mylius S. Systematic Hazard Analysis for Frontier AI using STPA[J]. arXiv preprint arXiv:2506.01782, 2025.
[16] SCHMIDT S, KLLN G C, MICHAEL K. Comparison of Hazard Analysis Methods with Regard to the Series Development of Autonomous Vehicles[C]//2019 IEEE Intelligent Transportation Systems Conference (ITSC).Auckland, New Zealand: IEEE, 2019.
[17] Elizebeth M J, Chen S, Badaoui H E, et al. Safety Analysis of eVTOL Operations based on STPA[J]. arXiv preprint arXiv:2510.09283, 2025.
[18] Park H, Kim J. STPA analysis for safe operation of maritime autonomous surface ship under degradation state[J]. Frontiers in Marine Science, 2025, 12: 1601515.
[19] Wong L, Pawlicki T. Facilitating the application of systems-theoretic process analysis in healthcare: creating control structures using process maps[J]. Risk Analysis, 2023, 43(12): 2411-2421.
[20] Koivisto P. Application of STPA in Probabilistic Risk Assessment of the Loviisa Nuclear Power Plant[J]. 2025.
[21] Suzuki W. Safety Analysis and Design Improvement for Semi-Automatic Train Operation (STO) in High-Speed Rail Using STPA[D]. Massachusetts Institute of Technology, 2025.
[22] Larit K, Zennir Y, Rodriguez M. Hazard Analysis with STPA Methods: Application to Mould Level Control Within Continuous Casting Free Stream Operations[J]. International Journal of Safety & Security Engineering, 2025, 15(4).

[23] Liu T. Safety analysis of Civil aviation Flight and UAV Operation based on STAMP/STPA[C]//E3S Web of Conferences. EDP Sciences, 2024, 512: 03033.
[24] Zhang J, Zhang S, Liang Z, et al. A risk assessment method based on DEMATEL-STPA and its application in safety risk evaluation of hydrogen refueling stations[J]. International Journal of Hydrogen Energy, 2024, 50: 889-902.
[25] Chen X, Wang J, Lv Y, et al. STPA-Guided SOTIF Assessment of Real-Time Autonomous Driving Behavior in Uncertain Environments[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2025.
[26] Ejaz M R, Chikonde M. STPA for Autonomous Vehicle Safety in Traffic Systems[J]. 2022.
[27] Özçetin O, Baştabak C, Tüfekçi S E, et al. STPA-Guided SOTIF Analysis of Adaptive Cruise Control with Scenario-Based Validation on CARLA[C]//2025 Innovations in Intelligent Systems and Applications Conference (ASYU). IEEE, 2025: 1-6.
[28] Zhao X X, Li J Q, Li Z T. A quantitative evaluation about the safety of intended functionality (SOTIF) for adaptive cruise control based on extension optimization[J]. Advances in Transportation Studies, 2025, 67.
[29] Soleimani M, Sari A A. A unified safety framework for automated vehicle development: integrating ISO 26262, SOTIF, and UL 4600[J]. Transportation Research Interdisciplinary Perspectives, 2026, 36: 101831.
[30] Chen X, Wang J, Lv Y, et al. STPA-Guided SOTIF Assessment of Real-Time Autonomous Driving Behavior in Uncertain Environments[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2025.
[31] Sun B, Yang S, Wang Y, et al. A fusion safety and security analysis framework for intelligent and connected vehicles[J]. PLoS One, 2025, 20(9): e0332050.

Yilin Zhong is the Vice President of the Automotive Engineering Research Institute of the BYD Group. His research areas include the development of key technologies for high-voltage systems in new energy vehicles, as well as the development of key technologies for highly integrated electronic and electrical architectures.

Jinxiang Fang is the Manager of the Software Security Development Department at the BYD Group's Automotive Engineering Research Institute. His research focuses on the establishment of security systems and capabilities for intelligent connected vehicles, as well as the application and regulation of vehicle big data.

Xiangjian Wang is the Section Chief of the Functional Safety Technology Division in the Software Security Development Department of the BYD Group. His research focuses on the development and evaluation of vehicle functional safety performance, MBSE-based digital design, and forward-looking technologies for safety integration.

Qingming Liu is an Engineer in the Functional Safety Technology Division of the BYD Group's Automotive Engineering Research Institute. His research focuses on the research and development of functional safety and safety of the intended functionality (SOTIF) for road vehicles, as well as multidimensional safety integration analysis methodologies based on STPA.

Yuanhao Meng is an Engineer in the Functional Safety Technology Division of the BYD Group's Automotive Engineering Research Institute. His research focuses on the application of MBSE in functional safety and STPA methodology.

Xiaoping Chen is a Senior Engineer at the BYD Group's Automotive Engineering Research Institute.

Her research focuses on MBSE methodology and the digital transformation of automotive research and development.