International Journal of Automotive Technology, Vol. ?, No. ?, pp. ?−?(year)

Serial#Given by KSAE

VISEF: EMPIRICAL EVALUATION OF A VEHICLE-LEVEL INTEGRATED FUNCTIONAL SAFETY FRAMEWORK

Taewan Gu*

Automotive R&D Division, Hyundai Motor Company, Hwaseong 18280, Korea

(*Received date ; Revised date ; Accepted date*) * Please leave blank

ABSTRACT− Modern vehicles operate as Systems of Systems, with tightly coupled interactions with many subsystems. As a result, traditional item-level safety analysis based on ISO 26262 often leads to redundant or omitted hazards, limiting the ability to assure comprehensive vehicle-level functional safety. This study proposes the Vehicle-level Integrated Functional Safety Framework (VISEF) to overcome these limitations by enabling holistic safety analysis across subsystems. VISEF consists of three key stages. First, a conventional item-level hazard identification and ASIL assignment process is conducted. Second, hazard integration is performed using functional, operational, and scenario-based similarity measures to identify and consolidate redundant hazards, followed by ASIL reallocation. Third, safety path inspection is applied by generalizing control flows between ECUs into structured input-processing-output streams. To validate the framework, a dual-pronged evaluation approach was employed. A nonlinear probabilistic saturation model was used to compare the system-level safety assurance probability before and after applying VISEF. Additionally, VISEF was applied to an actual commercial xEV truck/bus project. This study provides both experimental and empirical evidence that integrated vehicle-level hazard management contributes to system-level safety. VISEF offers a structured, scalable methodology for extending ISO 26262, and establishes a foundation for future standardization in vehicle-level functional safety engineering.

KEY WORDS : Vehicle-level functional safety, System of Systems (SoS), ISO 26262 extension, Hazard integration, ASIL reallocation, Safety path analysis, Functional safety inspection, ECU interaction safety, Automotive safety framework, xEV safety evaluation, ASIL inconsistency

1. INTRODUCTION

The modern automotive industry is rapidly evolving into a complex Cyber-Physical System (CPS), driven by advances in electric vehicles (xEVs), autonomous driving, and Software Defined Vehicles (SDVs) (de Oliveira, et al., 2024; Jiang). As a result, the number of Electronic Control Units (ECUs) in vehicles has surpassed 100, with each ECU becoming increasingly function-specific. Interactions among ECUs significantly affect overall vehicle behavior and safety, especially when safety-critical functions are distributed across multiple ECUs. In such cases, not only individual failures but also emergent hazards from inter-ECU interactions must be addressed (Kim, et al., 2025).
ISO 26262 is the international standard for functional safety in automotive systems (ISO 26262, 2018). It defines a lifecycle process for identifying hazards, determining Automotive Safety Integrity Levels (ASILs) and Safety Goals, and deriving Functional Safety Requirements (FSR). However, ISO 26262 is inherently item-centric, focusing on specific system units or functions. This leads to several limitations when attempting to ensure functional safety at the whole-vehicle level:

- Emergent hazards arising from interactions between systems may not be sufficiently identified through individual item-level analyses.
- Similar hazards may be redundantly defined across different items, leading to excessive safety requirements and increased development and validation costs.
- ASILs may be inconsistently or incompletely allocated across functional flows, compromising the integrity of the safety design.

These structural limitations become more pronounced in modern vehicles with highly integrated control systems and complex E/E architectures, emphasizing the need for

* *Corresponding author*. e-mail: taewan.gu@hyundai.com

a new analytical framework that considers the vehicle as a whole.

A real-world example is the vehicles between 2009 and 2011, where the U.S. National Highway Traffic Safety Administration (NHTSA) and National Aeronautics and Space Administration (NASA) concluded that the root cause was not individual ECU failures, but unexpected system interactions (Jim, et al., 2015). Despite the technical and structural challenges, a well-defined vehicle-level safety analysis framework that preserves the ISO 26262 structure while systematically managing redundant and missing hazards remains absent in both academia and industry. To address these challenges, this study proposes a vehicle-level integrated functional safety framework, named VISEF that treats the vehicle as a SoSSoS while adhering to the structure of ISO 26262 extending our previous work (Kim, et al., 2025).

The VISEF consists of the following three key procedures: (1) Item-level hazard identification based on ISO 26262, (2) Elimination of redundant hazards and derivation of integrated hazards based on functional, operational, and scenario similarity, and (3) Construction of vehicle-level safety paths and redefinition of vehicle-level safety goals through ASIL consistency assurance and reallocation.

The main contributions of this study are as follows: (1) A probabilistic simulation was conducted to evaluate the effectiveness of the proposed vehicle-level integrated functional safety framework. The simulation quantitatively verified improvements in safety assurance under varying levels of system complexity and risk. (2) To complement the simulation results and verify practical applicability, the framework was applied to real-world xEV truck and bus development projects and assessed using Delphi analysis by an expert group. (3) The study defined quantitative criteria for measuring functional, operational, and scenario similarity. Simulation results confirmed that these criteria are effective for identifying and removing redundant hazards defined across multiple ECUs. (4) An ASIL inspection method was developed to systematically detect omissions and inconsistencies in ASIL assignments along safety paths. The effectiveness of this detection method was validated through simulation. Finally, A Trajectory Matrix was constructed to structurally represent ASIL allocation across functional flows. This matrix served as a practical feedback mechanism, enabling identification of design areas requiring improvement.

The remainder of this paper is structured as follows: Section 2 defines the problem addressed in this study and highlights the structural limitations inherent in conventional ISO 26262-based approaches. Section 3 reviews ISO 26262-based safety analysis methods, the limitations of item-level assessment, and related studies aimed at achieving vehicle-level functional safety. Section 4 describes the proposed vehicle-level functional safety framework, detailing its structure and procedures, along with key criteria for redundancy elimination and ASIL consistency assurance. Section 5 establishes a system-theoretic definition to support simulation-based evaluation of the framework, followed by multi-dimensional assessments using simulation data and expert judgment. Section 6 discusses additional considerations, including internal and external validity threats and generalizability of the constructed concepts. Finally, Section 7 concludes the paper by summarizing the findings and outlining directions for future research and practical applications.

2. PROBLEM DEFINITION AND MOTIVATION

2.1. Structural Limitations of ISO 26262 and the Need for a Systems of Systems (SoS) Approach

Modern vehicle architectures have evolved into highly integrated systems where dozens of ECUs, sensors, and actuators cooperate to deliver functional performance. These architectures are best described as SoS, wherein complex and dynamic interactions are intrinsic to system behavior (Jamshidi, 2008).

However, the ISO 26262 standard, which is widely adopted for functional safety assurance, is fundamentally constructed around the concept of an "item"—a single function or logical unit. Each item independently undergoes Hazard Analysis and Risk Assessment (HARA) and is assigned ASILs accordingly. This item-centric approach presents critical limitations in SoS environments, particularly in the following aspects:

- Hazard Duplication: Similar or overlapping hazards may be defined redundantly across items due to independent HARA processes, resulting in excessive safety goals, unnecessary design constraints, and increased development costs.
- Hazard Omission: Emergent hazards that arise from dynamic interactions between multiple systems are often not captured in isolated item-level analyses.
- ASIL Inconsistency: Without a system-wide view, it becomes difficult to maintain ASIL consistency along functional or data flow paths that traverse multiple subsystems.
- No Formal Support for Integration or Reallocation: ISO 26262 provides no formal mechanism for integrated hazard redefinition, ASIL reallocation, or system-level safety path modeling.

These limitations are particularly problematic in high-dependency domains such as braking-steering-powertrain integration or autonomous driving, where a single failure can propagate rapidly and manifest as system-wide safety issues. Therefore, a shift is required toward a SoS based safety framework that models vehicle functions as interacting subsystems and explicitly identifies emergent hazards.

Such a framework must support integrated hazard identification, functional safety path derivation, and ASIL reallocation at the vehicle level, beyond the item-centric constraints of ISO 26262.

2.2. Lack of Practical Tools for Ensuring Traceability and Design Integration

In addition to the structural limitations discussed above, a critical and practical challenge exists in current safety engineering practices: there is no systematic method or tooling to verify whether the results of hazard analysis are consistently and correctly reflected in the actual system design. This disconnect often leads to safety mechanisms being either omitted or redundantly implemented, as there is a lack of formal mechanisms to trace safety goals back to their implementation in the system.

Furthermore, ASILs assigned at the output level are frequently found to be inconsistent with those at upstream inputs along the functional path, compromising system-wide safety integrity. To address these issues, there is a pressing need for a practical and structured safety inspection framework that enables:
- Mapping of safety paths across subsystems
- Verification of ASIL consistency along these paths
- Documentation of omissions and inconsistencies
- Feedback integration into design and architecture decisions.

In summary, ISO 26262's item-level focus is insufficient for ensuring comprehensive safety in modern vehicles, which are inherently structured as SoS.

To overcome this, there is a clear need for a vehicle-level integrated functional safety framework that integrates SoS modeling, interaction-based hazard identification, ASIL reallocation, and practical design traceability mechanisms.

3. REVIEW OF RELATED WORK

3.1. Functional Safety in SoS

Modern Traditional functional safety frameworks have largely focused on single vehicles or individual ECUs (Kovtun, et al., 2022; Ozirkovskyy, et al., 2022; Song, et al., 2024). However, modern vehicles increasingly adopt System of Systems (SoS) architectures, involving multiple subsystems (e.g., cooperative driving, V2X, advanced ADAS) interacting dynamically (Helmy, et al.; Lim, et al., 2024; Chen, et al., 2022). These interactions can lead to emergent hazards, which are difficult to identify through item-based analysis alone (Khabbaz Saberi, 2020; Lee, et al., 2014).

To ensure safety in SoS, structured modeling of interactions, synchronization mechanisms, and distributed responsibilities is essential. Several works have proposed model-based techniques tailored to these complex dependencies (Yuan, et al., 2024; Mudhivarthi, et al., 2023; Heithoff, et al., 2023; Khabbaz Saberi, 2020).

3.2. Extension of ISO 26262 to SoS Architecture

The ISO 26262 standard is designed primarily for safety assessments at the component or item level and does not readily address the complexity of SoS. Recent studies have proposed extending ISO 26262 by incorporating model-based safety lifecycle adaptations that reflect SoS-specific interaction hazards (Khabbaz Saberi, 2020; Kochanthara, et al., 2020).

In cooperative vehicle systems, safety goals and ASIL determinations vary by architecture type—Ad hoc, Centralized, or Hybrid—and require differentiated strategies for FSR validation and verification (Gharib, et al., 2019).

3.3. Safety Verification of Nonlinear Systems via Linerarization

Automotive SoS are inherently nonlinear systems. Various linearization-based verification methods have been developed to facilitate safety analysis. Carleman linearization allows for transforming nonlinear systems into infinite-dimensional linear systems, enabling reachable set computations and predictive control synthesis (Amini, et al., 2025).

Piecewise and partial feedback linearization techniques, combined with Control Barrier Functions (CBF), enable safety constraints enforcement even under real-time conditions in nonlinear environments (Cohen, et al., 2024; Arab, et al., 2024).

3.4. Limitations of Existing Approaches

Conventional ISO 26262 practices are limited by their item-centric scope, potentially leading to redundant or omitted hazards arising from subsystem interactions (Correa-Jullian, et al., 2024). Such limitations can result in misallocated ASIL levels and inflated safety requirements, increasing system complexity and cost.

Moreover, many linearization-based methods are computationally intensive and assume static system models, making real-time application difficult. In SoS, dynamic interconnections and uncertain transitions further complicate model fidelity and stability (Duggirala, et al., 2013).

3.5. Research Differentiation of This Study

This study is distinguished in the following aspects:

- SoS-Based Hazard Analysis Beyond Item-Centric Models: This research proposes a safety analysis framework that incorporates subsystem interaction models to identify emergent hazards at the vehicle level.
- Partial Linearization for Scalable Safety Verification: We adopt partial linearization techniques to enable computationally feasible safety verification in SoS with nonlinear interactions.
- ASIL Reallocation and Safety Path Integration: The framework includes hazard decomposition and ASIL reassignment mechanisms, followed by quantitative safety path analysis to validate and optimize FSR.

4. VISEF: A VEHICLE-LEVEL INTEGRATED FUNCTIONAL SAFETY FRAMEWORK BASED ON ISO 26262

Modern vehicle systems have evolved into SoS architectures, wherein dozens of ECUs interact in complex ways. However, ISO 26262 was designed for item-level safety assurance and structurally lacks the ability to comprehensively address emergent hazards arising from dynamic system interactions.

To address this limitation, this study proposes the VISEF, which preserves the foundational structure of ISO 26262 while enabling functional safety assurance at the whole-vehicle level.

As shown in Figure 1, this framework consists of the following three core stages:

4.1. Step 1: ECU-Level Hazard Identification

For each ECU, the ISO 26262 procedures—Item Definition, HARA, and FSR derivation—are performed. This assigns ASILs to each function and defines initial safety requirements. While this step adheres to ISO 26262's structured methodology, it also serves as the foundational input for the subsequent vehicle-level integration analysis.

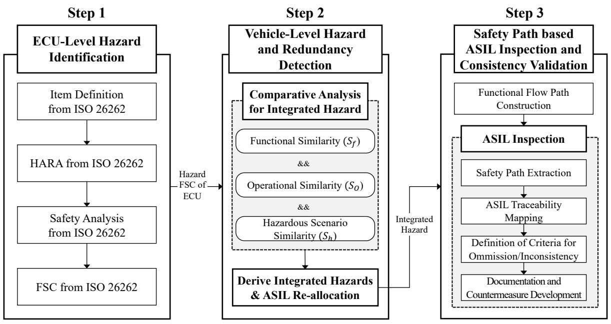

Figure 1. VISEF: Vehicle-Level Integrated Functional Safety Framework Overview.

4.2. Step 2: Vehicle Level Integrated Hazard Analysis

In Step 2, an integrability analysis is conducted based on the hazard lists identified at the ECU level. Three similarity metrics are defined – Functional Similarity, Operational Similarity, and Hazardous Scenario Similarity – and used to perform pairwise comparisons of hazards to identify candidates for integration. Hazards with high integratability are redefined into unified top-level hazards, and their ASIL levels are reassessed accordingly. This process serves as a core mechanism for redundancy elimination.

(1) Functional Similarity ($\boldsymbol{S_f}$)

Functional similarity measures the extent to which two subsystems share common control objectives or perform similar functions. It means they control identical or similar physical quantities (e.g., speed, angle, torque) and share analogous control objectives. This implies that a functional error in one subsystem can directly affect the other. For instance, if both the braking system and the powertrain system control vehicle speed, a malfunction in one could interfere with the other's control, leading to an integrated hazard that compromises vehicle stability.

$$S_f(A, B) = \frac{|F_A \cap F_B|}{|F_A \cup F_B|} \tag{1}$$

Where,

- F_A, F_B: Sets of functions performed by subsystems A and B
- $S_j \in [0, 1]$: A value of 1 indicates complete functional overlap

(2) Operational Similarity ($\boldsymbol{S_o}$)

Operational similarity quantifies the closeness of operating conditions under which two subsystems are active. It means that both subsystems can simultaneously experience stress or become vulnerable under specific circumstances. For example, when both emergency braking and sharp steering are required on a low-friction surface, both the braking and steering assist systems must operate at their limits. A minor error in one system during this process could impact the other's operation, leading to complex hazards like vehicle skidding.

$$S_o(A,B) = \frac{1}{1+\|\overrightarrow{C_A}-\overrightarrow{C_B}\|} \quad (2)$$

Where,

- $\overrightarrow{C_A}, \overrightarrow{C_B}$: Operational condition vectors (e.g., vehicle speed, road slope, environmental conditions)
- A smaller Euclidean distance implies higher operational similarity

(3) Hazardous Scenario Similarity (S_h)

Hazardous scenario similarity assesses whether two subsystems contribute to common or overlapping hazard outcomes (Top Events). It means two subsystems A and B share identical or analogous initial events, intermediate errors, and patterns that lead to the final hazard outcome.

This suggests that if a specific type of failure occurs in one subsystem, the other subsystem is also likely to fail sequentially or simultaneously due to a similar failure mechanism. For instance, if a sensor error can cause unintended braking in the braking system, a similar sensor error could affect the powertrain, leading to unintended deceleration.

$$S_h(A,B) = \frac{|H_A \cap H_B|}{|H_A \cup H_B|} \quad (3)$$

Where,

- H_A, H_B: Sets of hazardous scenarios originating from subsystems A and B
- High similarity indicates convergence to the same critical hazard or accident consequence

The integrated hazards derived from these criteria form the basis for redefining top-level vehicle safety goals. Through ASIL reallocation, system-wide safety consistency can be ensured.

By aggregating the three similarity metrics, an integration score ($\mathrm{R_{score}}$) is computed. If the score exceeds a predefined threshold (θ, we assume that θ = 0.75 in this study.), the hazards are redefined as a single integrated hazard.

$$\mathrm{R_{score}} = \mathrm{w_f S_f} + \mathrm{w_o S_o} + \mathrm{w_h S_h} \quad (4)$$

Where,

- $\mathrm{w_f}$, $\mathrm{w_o}$, $\mathrm{w_h}$: Weighting factors for functional, operational, and scenario similarity (as determined in consultation with domain experts)

4.3 Step 3: Safety Path-Based ASIL Inspection and Consistency Validation

The core of this framework is to clearly define the concept of a safety path – a functional flow trajectory associated with each integrated hazard and to verify ASIL consistency along this path. A safety path consists of a series of operational units connected via data and control flows between ECUs or software functions. It represents the propagation chain of safety–critical information across the system, which serves as a basis for hazard traceability and ASIL alignment. This structure can be mathematically formalized as follows:
The Safety Path $\mathcal{P}$ is a sequence of finite ordered triples:

$$\mathcal{P} = (x_0, f_0, y_0), (y_0, f_1, y_1), \ldots, (y_{n-1}, f_n, y_n) \quad (5)$$

Where,

- $x_0 \in X$: External or initial system input
- $f_i : X \longrightarrow Y$: Functional processing function (e.g., ECU control logic, middleware function)
- $y_i \in Y$: Output generated by the corresponding process f_i

This structure reflects a sequential input-process-output paradigm, where each process f_i is responsible for a functional transformation under safety constraints. In order to preserve safety integrity across the path, the following constraints must hold:

$$\forall i,\ ASIL(f_i) \geq ASIL(\mathcal{P}) \quad (6)$$

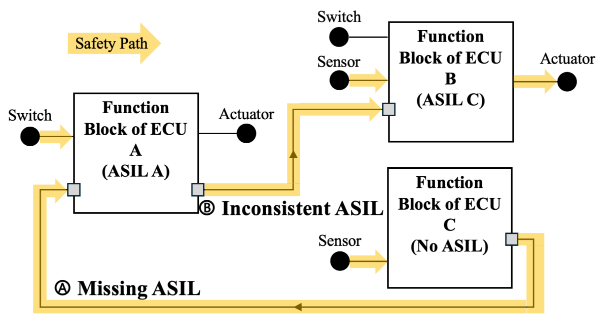

Figure 2. Example of Safety Path among ECUs.

That is, if the safety path $\mathcal{P}$ is associated with ASIL C, then all functional transformations f_i within the path must be compliant with at least ASIL C. If any function in the path fails to meet this criterion, the safety assurance of the overall path is compromised. Figure **2** shows a general example of the safety path among the ECUs.

To provide a concrete interpretation of this structure, we present an example of a safety path associated with the processing and propagation of vehicle speed data in an electronic braking system. The path can be represented as follows:

$$\mathcal{P}_{\text{speed}} = (\text{HRW}, f_{EBS}, v), (v, f_{VCU}, CCVS), (CCVS, f_{IBU}, Disp)$$

Where,
- *HRW*: Raw wheel speed data received by Electronic Braking System (EBS) from wheel sensors
- f_{EBS}: Function in the EBS that calculates vehicle speed from HRW
- v: Resultant vehicle speed
- f_{VCU}: Function in the Vehicle Control Unit (VCU) that converts speed into Cruise Control/Vehicle Speed (CCVS) format
- *CCVS*: Standardized speed format per J1939
- f_{IBU}: Function in the IBU that distributes speed to display or other subsystems
- *Disp*: Final output of the path, shown to the driver or forwarded to ADAS

Although the same "vehicle speed" data is propagated along this chain, each functional process f_i may be associated with different safety goals, resulting in non-uniform ASIL. For example, f_{EBS} may require ASIL C due to its control function, whereas f_{IBU} may only require ASIL B or even Quality Management (QM), depending on its role.

The VISEF framework extracts such as safety paths from the system model. It verifies that all f_i comply with or exceed the required ASIL, ensuring safety consistency and traceability across domains.

Subsequently, the ASIL inspection based on safety paths is performed according to the following activities:

(1) Safety Path Extraction
Based on Fault Tree Analysis (FTA)/Dependent Failure Analysis (DFA) results, analyze the system architecture, the input/output flows of each ECU to define function path and identify output functions assigned an ASIL, extract the safety relative functional flow directly connected to the hazard and model it as $\mathcal{P}$ using the above mathematical structure.

(2) ASIL Traceability Mapping
For each node f_i, input x_i, and output y_i, organize the assigned ASILs into a mapping table.
(3) Definition of Criteria for Omission/Inconsistency
- Omission (Missing): Some nodes in the path lack ASIL allocation
- Inconsistency: $ASIL(f_i) < ASIL(\mathcal{P})$ is not satisfied

(4) Documentation and Countermeasure Development
- ASIL readjustment, design of supplementary safety mechanisms
- Consideration of ASIL decomposition conditions
- Visualize and verify system-wide consistency safety mechanism design with Trajectory Matrix

Especially, the Trajectory Matrix quantitatively visualizes the ASIL assignment status between inputs and outputs, serving as a systematic tool for validating design quality and safety consistency.

4.4 Structural Differentiation and Practical Contributions of the Framework

While VISEF builds upon the ISO 26262 process, it structurally extends the analysis to the vehicle level as shown in Table 1.

Table 1. Comparison table between ISO 26262 approach and VISEF approach

Comparison	ISO 26262	VISEF
Analysis Scope	Item	Integrated Items (Vehicle level)
Hazard Analysis	Functions in an Item	Interactions among Items
Detection of Redundancy and Missing	Lack	Similarity based Quantitative Detection
ASIL Consistency	Within an Item	Safety Path based, Trajectory Matrix
Applicability to Real Project	Recommendation of Concept	Structured Framework and Methodology

4.5 Summary of the VISEF

VISEF enables structural risk analysis based on the integrated functional flow of the entire vehicle, going beyond functional safety at the single item level. By defining the safety path as a mathematically structured sequence of functions:
- Interactions between systems can be quantitatively represented
- ASIL consistency verification is systematized

5. VALIDATION OF THE PROPOSED FRAMEWORK

This section presents a two-layered validation strategy to evaluate the effectiveness of the proposed VISEF. The validation consists of:
(1) a quantitative simulation-based evaluation using a nonlinear probabilistic risk model, and
(2) an expert-driven empirical validation using the Delphi method.

The framework aims to reduce redundant safety requirements by integrating similar hazards and to improve system-level consistency by detecting missing or misaligned ASILs along safety paths. Each validation approach is designed to test these core objectives from different perspectives.

- In the simulation-based validation, the improvement in the probability of achieving safety goals before and after applying the framework is quantified using Monte Carlo simulations. This approach captures system-level risk behaviors under various conditions.
- In the expert-based validation, domain experts evaluate safety consistency and completeness through structured inspections along safety paths. The Delphi method ensures objectivity and convergence of expert judgments.

By combining both quantitative and qualitative evidence, this validation strategy substantiates the practical applicability and safety contribution of the VISEF framework.

5.1 Vehicle-Level Integrated Functional Safety Framework Modeling

This section mathematically models the effectiveness of the proposed framework and visualizes its behavior under different system conditions. The model treats the vehicle as a SoS, comprising interacting subsystems such as braking steering, and propulstion, each with its own hazards and safety mechanisms. Unlike traditional item-level approaches in ISO 26262, which often fail to capture interdependencies between ECUs, the proposed model represents system-level complexity by incorporating hazard interactions, ASIL consistency, and redundancy.

The P_{safe} is determined by the interaction of multiple system factors and cannot be expressed by a simple linear model. Therefore, this study defines a nonlinear function that reflects the contribution of each factor and models the saturation or reduction of effectiveness as complexity and risk increase:

$$P_{safe} = \tanh(Z) \cdot \left(1 - e^{(1-R_{veh})}\right) \quad (7)$$

where the internal score P_{safe} is defined as a weighted sum:

$$Z = \omega_1 \cdot H_{comp}^2 + \omega_2 \cdot \sqrt{E_{dom}} + \omega_3 \cdot \log(1 + I_{score}) + \omega_4 \cdot F_{struct}^2 - \omega_5 \cdot (C_{int} \cdot N_{sub})^{1.5} - \omega_6 \cdot R_{veh}^{1.5}$$

Variable definitions are described in Table 2.

Table 2. Probabilistic Model Variables

$H_{comp} \in [0,1]$	Completeness of item-level HARA execution
$E_{dom} \in [0,1]$	Domain expertise of participants
$I_{score} \in [0,1]$	Quality of interaction among multiple participants
$F_{struct} \in [0,1]$	Degree of framework structuring
$C_{int} \in [0,1]$	Interaction complexity among subsystems
$N_{sub} \in Z$	Number of subsystems
$R_{veh} \in [0,1]$	Vehicle-level risk without framework application
$\omega_1 \sim \omega_6$	Weight coefficients for each term (can be normalized)

Key features of the model include:
- Execution quality and domain expertise are reflected nonlinearly via exponential/logarithmic transformations.
- As system complexity and vehicle risk increase beyond certain thresholds, their effect reduces the overall effectiveness.
- The use of $\tanh(Z)$ and damping factors naturally expresses saturation and reduction zones in the model.

To evaluate the validity of the proposed model, simulations were performed across various system scenarios. The number of subsystems (N_{sub}) and vehicle-level risk (R_{veh}) were set as the main variables, while other factors were fixed as follows:

$$H_{comp} = 0.8, E_{dom} = 0.9, I_{score} = 0.7, F_{struct} = 0.85, C_{int} = 0.7$$

A total of 320 condition combinations were used to calculate P_{safe}, and the results were visualized as a three-dimensional surface graph. Figure 3 clearly shows how the framework's effectiveness varies under different conditions.
3D surface visualization of the framework's effectiveness (P_{safe}) by scenario: As the number of subsystems increases or vehicle-level risk rises, the effectiveness plateaus or decreases beyond a certain point.

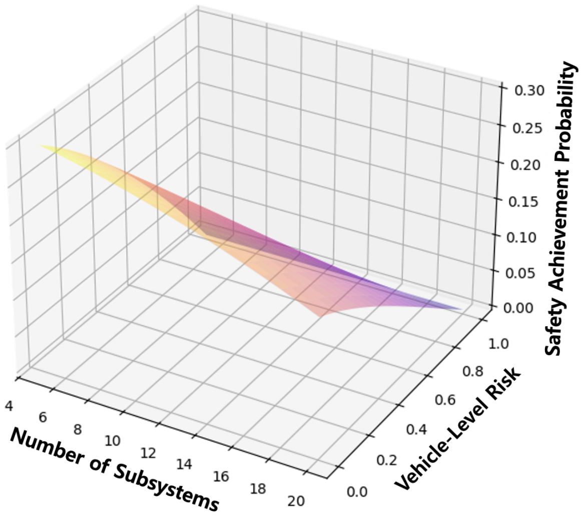

Figure 3. Example of the Vehicle-Level Safety Framework under Nonlinear Saturation Model.

The modeling results provide the following design insights: (1) Ensuring domain expertise and high-quality HARA execution significantly increases the effectiveness of the framework in the initial stages. (2) However, as system complexity and risk levels rise, the effectiveness saturates or decreases, indicating inherent limitations in achieving functional safety through structuring alone. (3) Therefore, to secure vehicle-level functional safety, strategies to reduce system complexity and design for risk mitigation must be implemented alongside structural improvements.

5.2 Simulation Analysis for Framework Validity

To demonstrate the effectiveness of the proposed vehicle-level functional safety framework, a quantitative experiment was conducted using a scenario-based Monte Carlo simulation integrated with a nonlinear saturation risk model. The objective of the simulation was to assess whether the application of the framework significantly improves the probability of achieving functional safety at the vehicle level.

The hypotheses are defined as follows:

- Null Hypothesis (H_0): Application of the framework does not have a significant effect on vehicle-level functional safety (i.e., there is no difference in the mean detection success rates between the two scenarios).
- Alternative Hypothesis (H_1): Application of the framework has a significant positive effect on functional safety (i.e., the detection success rate is significantly higher when the framework is applied).

To test this, a total of 10,000 Monte Carlo simulation trials were conducted. Each simulation compared the hazard detection success rates between the baseline (pre-framework) and the proposed (post-framework) scenarios. Probability distributions were applied based on a sigmoid risk function derived from system-level parameters. The threshold for success was defined as a hazard detection success rate greater than or equal to 0.8.

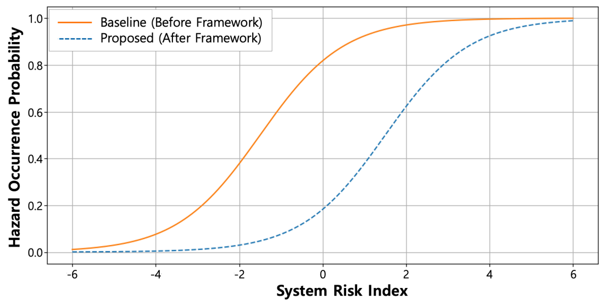

Figure 4. Hazard Occurrence Probability Curve Before and After Framework Application.

Figure 4 illustrates sigmoid-based hazard occurrence probability curves for both scenarios: with and without the proposed framework. The leftward shift of the curve in the proposed scenario indicates that hazard suppression is achieved more effectively at lower system risk levels, demonstrating the framework’s effectiveness in enhancing vehicle-level functional safety.

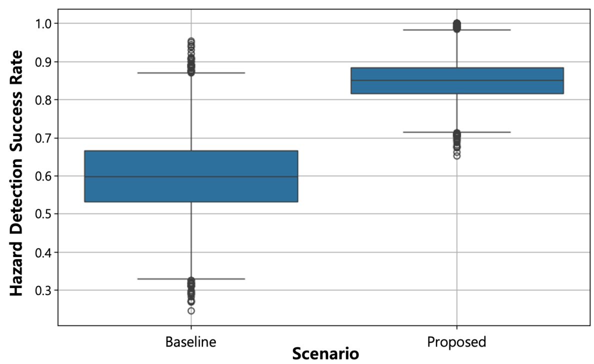

Figure 5. Comparison of Hazard Detection Success Rates Before and After Framework Application.

Figure 5 shows the distribution of hazard detection success rates from 10,000 Monte Carlo simulations for both scenarios. The proposed framework yields a higher median success rate and reduced variance, indicating improved reliability and robustness in hazard identification.

Table 3 provides the numerical results of the hypothesis test. The null hypothesis was strongly rejected ($p < 0.001$), supporting the claim that the framework contributes significantly to enhancing functional safety performance.

Table 3. Statistical Analysis Results

Test Method	Statistical Value	Description
T-Test	$p \approx 0.0000$	Significant difference in means (Reject H_0)
ANOVA	$p \approx 0.0000$	Significant difference in variances between groups
Fisher's Exact Test	$p = 0.0000$	Significant correlation between framework and success
Relative Risk (RR)	RR = 36.74	Success rate is 36.74 times higher with framework
Odds Ratio (OR)	OR = 226.19	Odds of success increase by 226 times (very large effect)

These results strongly reject the null hypothesis and statistically support the significant positive impact of the proposed framework on achieving functional safety.

In summary, this simulation study indicates that the VISEF framework enables more stable and consistent achievement of functional safety, especially under complex and high-risk conditions. The combination of the nonlinear risk function and repeated statistical simulation demonstrates a robust improvement, and the relative risk and odds ratio offer practical indicators for decision-makers. These results confirm the framework's value as a systematic approach to establishing safety in vehicle-level SoS architectures.

-

5.3 Framework Validity with Empirical Judgement

While the previous section 5.2 validated the effectiveness of the vehicle-level integrated functional safety framework through Monte Carlo simulations, simulation-based methods are inherently limited by assumptions regarding system structure and probability distributions. In particular, simulations may not fully capture issues such as omitted safety requirements or inappropriate ASIL allocations that arise in real systems with complex interactions. To address these limitations, this study employed an empirical validation approach based on the Delphi method involving domain experts.

The Delphi evaluation was centered on reviewing safety paths across the vehicle system. A safety path is defined as the functional flow from an ASIL-assigned output back to its originating inputs through interconnected control logic. To ensure consistency and objectivity, the following review criteria (Ground Rules) were established:

- Has functional safety analysis been performed for all data along the safety path?
- Are ASILs appropriately assigned to high-risk input signals?
- Are necessary safety mechanisms implemented without omission?
- Are there any inconsistencies between ASIL assignments for inputs and outputs?

Expert reviewers were asked to repeatedly score and refine their evaluations across three Delphi rounds until consensus was achieved. The target project was an xEV commercial vehicle involving braking, steering, and propulsion systems. Thirteen participants took part: five domain experts, five functional safety managers, and three facilitators. The evaluation period lasted from March to May 2025, and each item was rated using a 5-point Likert scale (1: very inappropriate, 5: very appropriate). Consensus was defined as a median score $\geq$ 4 and an interquartile range (IQR) $\leq$ 1.

The analysis results are summarized in Figure 6 and Table 4. Before framework application, most evaluation items showed low median scores and large variance, indicating inconsistent or insufficient implementation of safety measures. After framework application, the median scores improved to 4 or higher across all items, and the IQR values converged to within 1 point—demonstrating a statistically meaningful improvement and a high level of expert consensus.

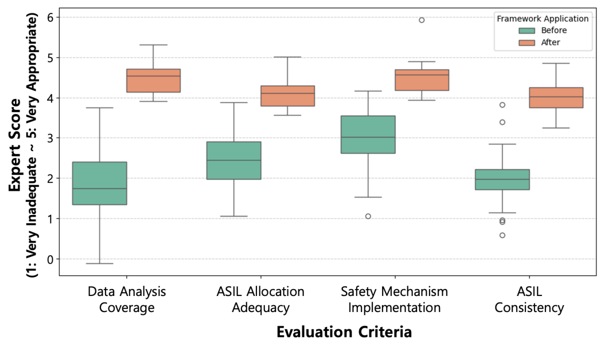

Figure 6. Expert Evaluation Results Based on Delphi Method. (Before and After Framework Application)

According to the panel's qualitative judgment, the framework significantly enhances the completeness and consistency of safety analysis by enforcing a structured review of safety paths. The approach proved effective in identifying omitted safety requirements and inconsistencies in ASIL assignment, particularly across system boundaries where traditional ISO 26262 item-level reviews fall short.

Table 4. Result of Qualitative Judgement of the Expert Panel

Item	Before Framework (Median ± IQR)	After Framework (Median ± IQR)
Data Analysis Ommission Rate	2.0 ± 1.5	4.5 ± 0.5
Appropriateness of ASIL	2.5 ± 1.0	4.0 ± 0.5
Adequacy of Safety Mechanism Implementation	3.0 ± 1.0	4.5 ± 0.5
ASIL Consistency	2.0 ± 1.0	4.0 ± 0.5

The Delphi evaluation provided empirical evidence that complements the simulation results. Notably, it revealed that the VISEF framework is not only theoretically valid but also practically applicable in real-world vehicle development projects. Furthermore, the structured inspection method and consensus-based feedback process suggest the framework's potential utility in future safety standardization and automotive industry practices.

5.4 Framework Effectiveness: Redundancy Perspective

This section evaluates how effectively the proposed VISEF reduces redundant safety requirements by integrating hazards that are functionally, operationally, or scenariowise similar. Redundancy is a known issue in ISO 26262 item-based hazard identification, especially when different suppliers or teams independently perform HARA. The VISEF framework addresses this by establishing clear criteria for hazard integration.

Hazards are considered integrable when satisfy all three of the following similarity conditions:

- Functional Similarity (S_f): Quantified as the ratio of shared functional aspects between two hazards based on the Jaccard similarity.
- Operational Similarity (S_o): Simulated to represent similarity between hazards occurring under the same driving situations and environmental conditions.
- Scenario Similarity (S_h): Evaluated based on the overlap of core events in scenarios to assess whether two hazards lead to the same Top Event.

Each metric ranges from 0 to 1, and integration is decided by the condition:

$$R_{score} \text{ if and only if } S_f \geq \theta_f \text{ and } S_o \geq \theta_o \text{ and } S_h \geq \theta_h$$

As we mentioned in previous section 4, each θ_f, θ_o *and* θ_h are assumed 0.75 in this validation.

Each hazard is considered a single safety requirement, and when redundant hazards are integrated, the number of requirements decreases, thereby reducing uncertainty within the system. To quantify this, the concept of Information Entropy was applied. Given the probability p that a requirement is unmet, the total entropy (H) for n requirements is:

$$H = n \times -p \log_2 p - (1-p) \log_2 (1-p)$$

In this simulation, p was set to 0.5 to represent maximum uncertainty.

A Monte Carlo simulation was conducted over 10,000 iterations. In each iteration, 20 hazards were randomly generated and evaluated for pairwise integration based on the similarity conditions. Every time a hazard pair met the integration threshold, the total number of requirements was reduced by one. Entropy before and after integration was calculated for each iteration.

The hypothesis test was defined as follows:

- Null Hypothesis (H_0): There is no statistically significant difference in the number of requirements and information entropy before and after hazard integration.
- Alternative Hypothesis (H_1): The number of requirements and information entropy significantly decrease after hazard integration.

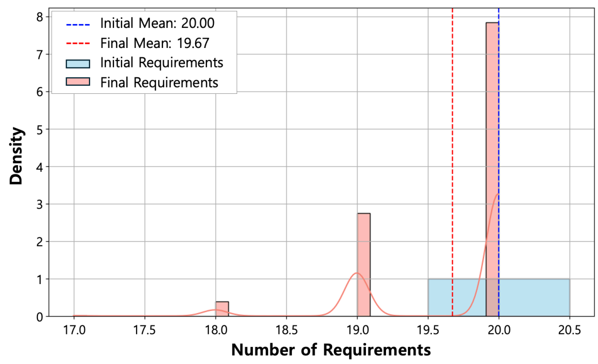

Figure 7. Distribution of Requirements Before and After Integration.

Figure 7 illustrates the distribution of safety requirements before and after hazard integration across 10,000 Monte Carlo trials. The blue histogram represents the initial number of hazards (each considered as an independent safety requirement), while the red histogram shows the final count after applying the proposed similarity-based integration framework. On average, the number of requirements decreased from 20.00 to approximately 19.67, reflecting the elimination of redundant hazards. The mean difference was statistically significant (paired t-test: $t = 59.45$, $p < 0.0001$), confirming that the proposed method effectively reduces requirement redundancy.

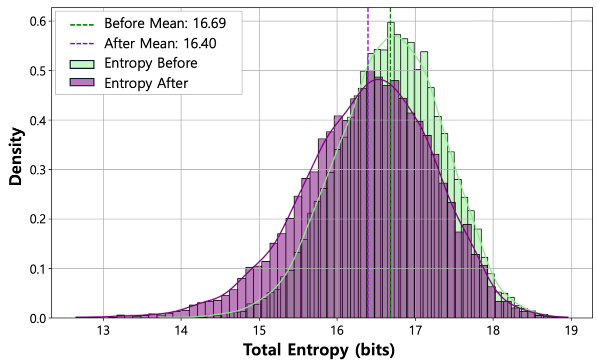

Figure 8. Distribution of Information Entropy Before and After Integration.

Figure 8 compares the system-level information entropy before and after hazard integration. Entropy was computed based on the probability of requirement violation (risk-weighted), using a nonuniform distribution of $p_i \in [0.1,0.9]$ for each hazard. The green histogram denotes entropy prior to integration, while the purple histogram indicates entropy after integration, including adjusted risk probabilities for merged hazards. The average total entropy decreased from 16.69 to 16.40 bits, demonstrating a statistically significant reduction in uncertainty (t = 58.36, p < 0.0001). This supports the hypothesis that the framework not only reduces the number of safety requirements but also enhances their clarity and determinism.

These results indicate that the VISEF framework not only reduces the count of safety requirements but also enhances their clarity and determinism by reducing uncertainty in the system. Furthermore, a strong linear correlation was observed between the number of integrated hazard pairs and the reduction in both requirement count and entropy, suggesting that the framework operates systematically to eliminate redundancy based on interpretable similarity metrics.
In the context of functional safety, information entropy serves as an abstract representation of system uncertainty in hazard handling. A higher entropy value indicates that the safety architecture contains many fragmented or redundant requirements, which can obscure traceability, complicate verification, and increase the likelihood of coverage gaps. By contrast, lower entropy reflects a more deterministic and streamlined safety structure, where each requirement is meaningful, distinct, and effectively mapped to a traceable hazard.

Therefore, the reduction in information entropy observed in our simulation is not merely a numerical improvement but a qualitative enhancement in system-level safety assurance. It suggests that the proposed VISEF framework promotes better clarity, alignment, and auditability in the safety lifecycle, ultimately contributing to more robust risk mitigation and compliance with ISO 26262 objectives.

5.5 Framework Effectiveness: Inconsistency

The vehicle-level integrated functional safety framework proposed in this study focuses on structurally identifying ASIL inconsistencies, under- or over-assessments, and omissions in HARA by tracing related input signals based on the ASIL assigned to the terminal output of the function path and quantitatively reviewing the ASIL assignment status for those inputs. To this end, an inspection based on the safety path was conducted, and the results were visualized using a Trajectory Matrix.

As a practical example, a functional safety review was performed on the braking control system of an electric commercial vehicle. Table 5 shows partial trajectory matrix of this study, which was constructed based on the existing HARA execution status, ASIL assignment levels, and functional contributions of these signals. The trajectory matrix-based inspection procedure proposed in this study was extended beyond the review of single functional flows to comprehensively cover the braking, steering, and propulsion domain controllers of an actual vehicle. Inspection was conducted across 87 input signals and 22 major output functions spanning three domains. As a result, a total of 29 cases of ASIL inconsistency were identified—issues that could not have been detected using conventional HARA-based approaches alone. The detailed findings are as follows:

- Underestimated cases: 11 (input ASIL rated lower than required by output)
- Overestimated cases: 9 (ASIL assigned excessively high relative to input)
- Missing ASIL cases: 6 (inputs without any ASIL assignment)
- Functionally irrelevant inputs: 3 (signals included unnecessarily in the safety path)

These results highlight the significant value of the proposed framework in identifying structural safety vulnerabilities at the vehicle system level—vulnerabilities that are often overlooked by traditional item-level approaches under ISO 26262. In particular,

Table 5. Partial Case of Trajectory Matrix from Real Project (xEV Truck/Bus)

No	Components	Functions	Relatives	Expected ASIL	Real ASIL
1	ECU A	Safety Warning (Tx)	ECU B	D	B
2	ECU C	Accel Pedal Sensor (Rx)	ECU D	QM	B
3	ECU C	Motoring Torque (Rx)	ECU D	D	C
4	ECU C	Driving Resistance (Rx)	ECU D	C	D
5	ECU C	Retarder Braking Torque (Rx)	ECU E	C	D
6	ECU C	Retarder Braking Torque (Rx)	ECU G	C	D
7	ECU F	Ignition Signal (Rx)	ECU D	B	QM
8	ECU F	EV Mode Information (Rx)	ECU D	B	QM
9	ECU F	Steering Angle (Rx)	ECU J	B	B
10	ECU H	Vehicle Speed (Rx)	ECU C	D	C
11	ECU H	Vehicle Speed (Rx)	ECU C	D	B
12	ECU H	Vehicle Speed (Rx)	ECU K	D	B
13	ECU H	Vehicle Speed (Rx)	ECU D	D	B
14	ECU H	Vehicle Speed (Rx)	ECU L	D	B
15	ECU I	Transmission (Rx) with ASIL	ECU C	D	QM
16	ECU I	Foundation Brake Usage (Rx)	ECU C	B	QM
17	ECU I	Actual Retarder Percent Torque (Rx)	ECU G	B	QM
18	ECU I	Stop Lamp On Request	ECU D	B	QM
19	ECU I	Actual Retarder Percent Torque (Rx)	ECU L	B	QM
20	ECU I	Head Lamp High On Request (Rx)	ECU N	A	A
21	ECU I	Wiper Out (Rx)	ECU N	A	A
22	ECU I	Head Lamp Low On Request (Rx)	ECU N	B	A
23	ECU I	Turn Signal Left Switch (Rx)	ECU O	A	B
24	ECU I	Turn Signal Right Switch (Rx)	ECU O	A	B
25	ECU M	Transmission (Rx) with ASIL	ECU C	D	QM
26	ECU M	Steering Angle (Rx)	ECU J	D	B
27	ECU M	Steering Angle (Rx)	Sensor	D	B
28	ECU M	Engine Speed (Rx)	ECU L	D	B
29	ECU M	Vehicle Speed (Rx)	ECU C	D	C

when multiple controllers within the system share data across functional boundaries, ASIL consistency is frequently compromised. The proposed framework provides a systematic analysis structure capable of detecting such inconsistencies.

It is noteworthy that this inspection process was not based on subjective qualitative judgments but was instead conducted using a predefined checklist designed for Trajectory Matrix construction as shown in Table 6. This checklist, comprising 12 items, systematically covers aspects such as analysis of the functional contribution of input signals, verification of HARA execution, assessment of ASIL consistency, domain expert review, and filtering of unnecessary signals. As a result, it played a decisive role in ensuring the objectivity and repeatability of the inspection process.

Table 6. Checklist for Trajectory Matrix

No	Inspection Item	Description	Verification Result
1	Is the output function clearly defined?	Is the output function at the end of the functional path specially described? (e.g., vehicle deceleration command, steering angle control, etc.)	
2	Are HARA results and ASIL defined for the output?	Are quantitative/qualitative HARA results and ASIL assigned for the output function?	
3	Are all input signals affecting the output sufficiently identified through backtracking?	Have all input signals been identified without omission? (Using design documents, functional specifications, signal interface documents, etc.)	
4	Has the functional contribution (impact) of each input signal been analyzed?	Has the impact of each input on the output been analyzed? (Rated as High/Medium/Low, etc.)	
5	Has it been confirmed whether HARA has been performed for each input signal?	Is there confirmation of whether HARA was performed for each signal, and are the results available?	
6	Is ASIL clearly assigned to each input signal?	Is the ASIL assigned to each input according to ISO 26262 (including A~D or QM)?	
7	Has consistency between output ASIL and input ASIL been reviewed?	Has inconsistency (underestimation, overestimation, omission) been analyzed between output and input ASIL?	
8	Has a domain expert review been conducted for ASIL inconsistencies?	Has a review been performed with the Functional Safety Manager or system architect?	
9	Has the need for adjustment (re-analysis, ASIL revision, diagnostic enhancement, etc.) been identified?	Are follow-up actions or recommendations confirmed for inconsistency items?	
10	Are all items required for constructing the Trajectory Matrix (signal name, impact, ASIL, etc.) organized?	Is the final matrix ready for compilation? (Organized in tabular format)	
11	Are unnecessary or unrelated input signals excluded from the safety path?	If inputs unrelated to ASIL are included, have exclusion measures been taken?	
12	Is it possible to visualize and calculate indicators based on input-output mapping information?	Is the structure complete for generating heatmaps, boxplots, ESR/IAC calculations, etc.?	

Furthermore, all 29 identified inconsistency cases were confirmed by domain experts to require design improvements. Some cases led to the insertion of diagnostic functions, re-execution of HARA, or reassignment of ASIL, resulting in concrete design changes. This demonstrates that the inspection process is not merely a review tool, but a practical means to enhance design quality and strengthen safety certification readiness in actual development environments.

6. THREAT TO VALIDITY

This study validated the proposed vehicle-level integrated functional safety framework using both quantitative simulations and qualitative expert evaluations (via the Delphi method). However, several threats to validity must be acknowledged, which may affect the generalizability and reproducibility of the findings.

First, some assumptions used in the simulation model—particularly the probabilistic variables and the nonlinear risk filter function—are simplifications of the complex interactions found in real-world vehicle systems. Specifically, the probability distributions for hazard duplication and omission were initialized using empirical data and analogous project cases. Nevertheless, these assumptions currently lack formal standardization and require iterative refinement through application in multiple real-world projects. Thus, the consistency and sensitivity of these variable settings must be continually improved through expanded empirical validation.

Second, the Delphi method inherently involves expert judgments, which introduces a degree of subjectivity.

Although the expert panel was carefully composed of domain experts and functional safety managers, and multiple rounds of consensus building were performed, it is not entirely possible to eliminate potential biases stemming from the specific composition of the expert group.

Third, the application scope of this study was limited to the braking, steering, and propulsion domains of electric commercial trucks and buses. The framework has not yet been validated for other vehicle systems (e.g., infotainment, energy management) or for passenger vehicle platforms. As such, further evaluation across a broader range of vehicle types and operational scenarios is essential to support the framework's generalizability. While these threats represent limitations of the present study, they also offer a foundation for further research and iterative refinement for practical deployment.

7. CONCLUSION

This study addressed the limitations of ISO 26262's item-level ASIL assignment in capturing cross-domain safety issues in modern SoS vehicles. To overcome these limitations, we proposed the VISEF, which enables hazard integration, ASIL consistency verification, and feedback-driven improvement through a structured trajectory matrix.

The framework was validated through Monte Carlo simulation and Delphi expert review. Simulation results confirmed a significant increase in the probability of achieving system-level functional safety. Expert-based evaluation further demonstrated VISEF's ability to detect overlooked ASIL inconsistencies in actual xEV control domains.

In summary, VISEF extends ISO 26262 with a practical and scalable approach that improves the consistency, traceability, and completeness of functional safety assurance in vehicle development.

Future work will focus on expanding VISEF's applicability through integrated vehicle-level testing to further validate its effectiveness under real-world conditions. In addition, we plan to develop algorithms for the automation of ASIL reallocation and the optimization of safety paths, enabling more efficient and adaptive safety design for complex systems. These enhancements are expected to strengthen VISEF's role as a foundational methodology for next-generation vehicle safety engineering.

REFERENCES

Amini Arash [et al.] Carleman linearization of nonlinear systems and its finite-section approximations [Journal] // Discrete and Continuous Dynamical Systems - B (DOI: 10.3934/dcdsb.2024102). - 2025. - 2 : Vol. 30. - pp. 577-603.

Arab Aliasghar [et al.] Safety Prioritization by Iterative Feedback Linearization Control for Collaborative Robots [Conference] // 2024 IEEE Conference on Control Technology and Applications (CCTA). - 2024.

Chen Sihan [et al.] MMTP: Multi-Modal Trajectory Prediction with Interaction Attention and Adaptive Task Weighting [Conference] // 2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC). - 2022.

Cohen Max H., Cosner Ryan K. and Ames Aaron D. Constructive Safety-Critical Control: Synthesizing Control Barrier Functions for Partially Feedback Linearizable Systems [Journal] // IEEE Control Systems Letters. - 2024. - Vol. 8. - pp. 2229-2234.

Correa-Jullian Camila, Ramos Marilia and Ma Jiaqi Operational safety hazard identification methodology for automated driving systems fleets [Journal] // Journal of Risk and Reliability (https://doi.org/10.1177/1748006X241233863). - 2024. - 2 : Vol. 239.

de Oliveira Vitor Furlan [et al.] Digital Twin and Cyber-Physical System Integration in Commercial Vehicles: Latest Concepts, Challenges and Opportunities [Journal] // IEEE Transactions on Intelligent Vehicles. - 2024. - 4 : Vol. 9. - pp. 4804-4819.

Duggirala Parasara Sridhar and Tiwari Ashish Safety verification for linear systems [Conference] // 2013 Proceedings of the International Conference on Embedded Software (EMSOFT). - 2013.

Gharib Mohamad [et al.] Engineering Functional Safety Requirements for Automotive Systems: A Cyber-Physical-Social Approach [Conference] // 2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE). - 2019.

Heithoff Malte [et al.] Challenges of Integrating Model-Based Digital Twins for Vehicle Diagnosis [Conference] // 2023 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C). - 2023.

Helmy Mona [et al.] ADAS System Integrated with New Architecture for V2X in Adaptive AUTOSAR [Conference] // 2023 International Telecommunications Conference (ITC-Egypt).

ISO 26262 Road Vehicles - Functional Safety. - 2018.

Jamshidi Mo Introduction to System of Sytems [Book Section] // System of Systems Engineering. - [s.l.] :

CRC Press, 2008.
Jiang Shugang Vehicle E/E Architecture and Key Technologies Enabling Software-Defined Vehicle [Conference] // WCX SAE World Congress Experience 2024 (https://doi.org/10.4271/2024-01-2035.).
Jim Sysko and Shinde Jaysinha S. Crisis Management at Toyota [Journal] // Advances in Management. - 2015. - 12 : Vol. 8. - pp. 16-21.
Khabbaz Saberi A Functional Safety: A New Architectural Perspective: Model-Based Safety Engineering for Automated Driving Systems [Book]. - [s.l.] : Mathematics and Computer Science]. Eindhoven University of Technology, 2020.
Kim Hyunsung [et al.] Vehicle Level Functional Safety Framework for ASIL Re-Allocation and Safety Confirmation [Conference] // KSAE 2025 Annual Spring Conference. - 2025.
Kochanthara Sangeeth [et al.] Semi-automatic Architectural Suggestions for the Functional Safety of Cooperative Driving Systems [Conference] // 2020 IEEE International Conference on Software Architecture Companion (ICSA-C). - 2020.
Kovtun Viacheslav, Izonin Ivan and Gregus Michal The Functional Safety Assessment of Cyber-Physical System Operation Process described by Markov Chain [Journal] // Sci Rep (DOI: https://doi.org/10.1038/s41598-022-11193-w). - 2022. - Vol. 12. - pp. 70-89.
Lee K. J. [et al.] Approach to functional safety-compliant ECU design for electro-mechanical brake systems [Journal] // International Journal of Automotive Technology(IJAT). - 2014. - Vol. 15. - pp. 325-332.
Lim Seongmook and Sung Kyungmo A Study on V2X Communication System Test Strategy using ASPICE and ISO 26262 [Conference] // 2024 15th International Conference on Information and Communication Technology Convergence (ICTC). - 2024.
Mudhivarthi Bhavesh Raju [et al.] Model Based Design in Automotive Open System Architecture [Conference] // 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS). - 2023.
Ozirkovskyy Leonid [et al.] Functional safety analysis of safety-critical system using state transition diagram [Journal] // Radioelectronic and Computer Systems (DOI: https://doi.org/10.32620/reks.2022.2.12). - 2022. - Vol. 2.
Song Haifeng [et al.] Functional Safety and Performance Analysis of Autonomous Route Management for Autonomous Train Control System [Journal] // IEEE Transactions on Intelligent Transportation Systems (DOI: 10.1109/TITS.2024.3402435). - 2024. - 10 : Vol. 25. - pp. 13291-13304.
Yuan Leidong [et al.] Research and Implementation on Dependency Relationship for Power Supply Reliability Management in Photovoltaic-Storage-Charging Station System Based on Complex Risk Model [Conference] // 2024 7th International Conference on Renewable Energy and Power Engineering (REPE). - 2024.