

Article

A Simulation-Based Approach to ASIL Determination for Longitudinal Motion Hazards Using Combined Operational Situations

Nikita Morozov , Stefan Pischinger  and Marco Günther 

Chair of Thermodynamics of Mobile Energy Conversion Systems, RWTH Aachen University, 52074 Aachen, Germany; pischinger_s@tme.rwth-aachen.de (S.P.); marco.guenther@tme.rwth-aachen.de (M.G.)

* Correspondence: morozov@tme.rwth-aachen.de

Abstract

With the increasing complexity of electrical and electronic (E/E) components in modern powertrains, functional safety requires more systematic assessment methods. This paper presents a simulation-based approach for automated Hazard Analysis and Risk Assessment (HARA) of battery electric vehicles in accordance with ISO 26262. The method combines operational-situation parameters, including vehicle speed, road surface, vehicle gap, and road inclination, to define a structured set of hazardous events. Severity, Exposure, and Controllability are evaluated using rule-based criteria, including a dedicated Controllability rule set for longitudinal motion hazards. Quantitative erroneous acceleration and deceleration thresholds associated with different ASILs are derived using a bisection search algorithm, enabling quantifiable and testable safety goals. Comparison with manual HARA reveals systematic biases: low speed does not necessarily imply improved Controllability due to shorter vehicle gaps, while Severity may be underestimated at low speeds because of high instantaneous electric-machine torque. The maximum ASIL is often identified similarly by simulation and experts, whereas lower-ASIL hazardous events may lack consistency and coverage in manual HARA. As a practical application, the approach can be integrated into existing automotive safety workflows as a HARA support tool, improving the consistency of lower-ASIL events while allowing engineers to focus on maximum ASIL cases.

Keywords: functional safety; ISO 26262; automotive; HARA; hazard; ASIL; hazard analysis; risk assessment



Academic Editor: Michael Fowler

Received: 29 May 2026

Revised: 17 July 2026

Accepted: 17 July 2026

Published: 19 July 2026

Copyright: © 2026 by the authors.

Published by MDPI on behalf of the World Electric Vehicle Association.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Functional safety has become a fundamental aspect of modern automotive development, driven by the increasing complexity of electrical and electronic (E/E) systems. The current state of the art is defined by ISO 26262 (latest edition 2018) [1], which establishes a comprehensive framework for ensuring functional safety throughout the entire vehicle lifecycle. Central to this framework is the dedicated safety V-cycle, which complements the conventional development process and ensures systematic consideration of functional safety from concept to production and operation.

At the concept phase, Hazard Analysis and Risk Assessment (HARA) plays a key role in identifying potential hazards, estimating associated risks, and determining the required Automotive Safety Integrity Levels (ASILs). These ASILs directly influence the

necessary safety measures and development effort, making HARA a critical starting point for safety-driven system design.

Functional safety considerations are particularly important for battery electric vehicles (BEVs), where new types of hazards arise due to high-voltage battery systems, electric drive units, and their associated thermal management systems. In the context of motion-related hazards, electric powertrains differ fundamentally from conventional combustion engine systems. Electric motors can generate both high positive and negative torque almost instantaneously over a wide operating range, whereas combustion engines provide only limited negative torque beyond passive drag. Consequently, HARA for BEVs must explicitly account for the possibility of unintended and uncontrolled application of both positive (acceleration) and negative (deceleration) torque.

There is a high level of complexity arising from numerous hazards and operational situations, each of which is traditionally assessed manually. This can lead to inconsistencies due to incomplete coverage of operational situations, insufficient consideration of relevant powertrain parameters, and consequently inaccurate ASIL determination. In addition, the process frequently relies on expert-based assessment methods with limited support from quantitative or data-driven evaluation metrics. As a result, analysts tend to assess hazards conservatively, which can lead to over-specified safety requirements [2]. Furthermore, various capabilities of different vehicle platforms cannot be adequately assessed through manual analysis. For instance, the torque–speed characteristics of electric machines in BEVs typically exhibit decreasing maximum torque at higher speeds, which can limit the magnitude of unintended torque and thereby influence the criticality of certain hazardous events. Such effects are usually not considered in manually performed HARA, which may lead to an overestimation of ASIL. To address these limitations and improve repeatability and consistency, data-driven, simulation-based HARA approaches have been introduced. However, they predominantly focus on lateral hazards [3] or automated driving functions [4,5], particularly addressing insufficient vehicle deceleration. Furthermore, some of these approaches focus only on operational situations with high exposure in order to target the highest ASIL classifications [6]. Other approaches simplify the assessment of driver interaction and mitigation potential by conservatively assuming worst-case conditions [7]. In addition, some methods rely on detailed vehicle parameters and the availability of high-fidelity vehicle models [8]. Consequently, such simulation-intensive approaches are mainly suited to later development stages when detailed system parameters are available, supporting re-evaluation and refinement of existing ASIL. Furthermore, emerging artificial intelligence (AI)-based approaches, particularly those using generative AI, may offer promising opportunities for ASIL determination [9,10]. However, such methods often require large representative datasets, may provide limited transparency, and can be difficult to justify in the context of ISO 26262.

This paper addresses the identified limitations by proposing a methodology for the automated HARA of longitudinal motion hazards, such as unintended acceleration and deceleration, which are often neglected in simulation-based analyses despite their varying ASIL classifications reported in the literature [11–13]. The approach combines multiple operational situations to ensure comprehensive coverage of relevant driving conditions and their interactions and introduces rule-based evaluation of all relevant ASIL-determining parameters. Vehicle behavior is simulated in MATLAB/Simulink 2025b under both nominal and fault conditions, including diverse fault injections with varying torque levels, rather than assuming only maximum torque. The proposed method explicitly quantifies erroneous acceleration and deceleration, extending the analysis beyond conventional ASIL classification. Furthermore, the approach is applica-

ble both to the entire powertrain and to individual vehicle functions with a restricted Operational Design Domain (ODD).

The main contributions of this paper are:

- A simulation-based approach for automated HARA of longitudinal motion hazards in BEVs, enabling consistent and structured analysis across the entire HARA.
- A rule-based evaluation of ASIL-determining parameters.
- Identification of erroneous acceleration and deceleration, leading to distinct ASIL classifications.

This represents a methodological advancement in HARA because the analysis is not limited to a small number of critical operational situations. Instead, a large number of hazardous events are assessed consistently across multiple scenario parameters, ensuring that the impact of each factor is considered throughout the HARA. By combining transparent rule-based ASIL evaluation with bisection-based estimation of acceleration and deceleration thresholds, the proposed approach enables a broader and more reproducible assessment than is typically achieved in manual HARA. It also differs from existing simulation-based approaches by not being restricted to selected operational situations, conservative worst-case assumptions, or detailed vehicle models. This makes it particularly relevant to early concept phases, enabling an initial assessment of hazard criticality and associated vehicle dynamics. Furthermore, unlike data-driven and AI-assisted methods, it does not require representative training datasets and retains deterministic and traceable assessment logic.

This paper is structured as follows. Section 2 provides the necessary background on ISO 26262, with a focus on HARA and the relevant ASIL-determining parameters. It also reviews existing research on the estimation of these parameters in simulation-based approaches. Section 3 presents the proposed methodology. Section 4 applies the approach to two BEVs of different performance classes, namely the Tesla Model 3 and the Volkswagen ID.3 and analyzes the results in comparison with literature values. Section 5 demonstrates the application of the approach to selected vehicle function with a restricted ODD, such as traffic jam assist, highlighting its support in defining functional limitations and ODD boundaries. Section 6 discusses the main biases and inconsistencies identified through the comparison between manual HARA and simulation-based HARA, examines the advantages and limitations of the proposed approach, and discusses its integration into existing automotive safety workflows. Section 7 concludes the paper by summarizing the main findings and contributions and outlining directions for future work.

2. State of the Art

In this section, the relevant background is presented. First, the ISO 26262 standard is introduced, and the relevant concepts and clauses related to HARA and ASIL determination are described. Subsequently, methods for estimating ASIL-determining parameters are reviewed.

2.1. Functional Safety for Road Vehicles

ISO 26262 addresses the functional safety of E/E systems in road vehicles across the entire product lifecycle, from concept to decommissioning. A key activity in the concept phase is HARA, which systematically identifies hazards, evaluates relevant operational situations, and assesses the associated risks. Figure 1 illustrates the overall HARA process.

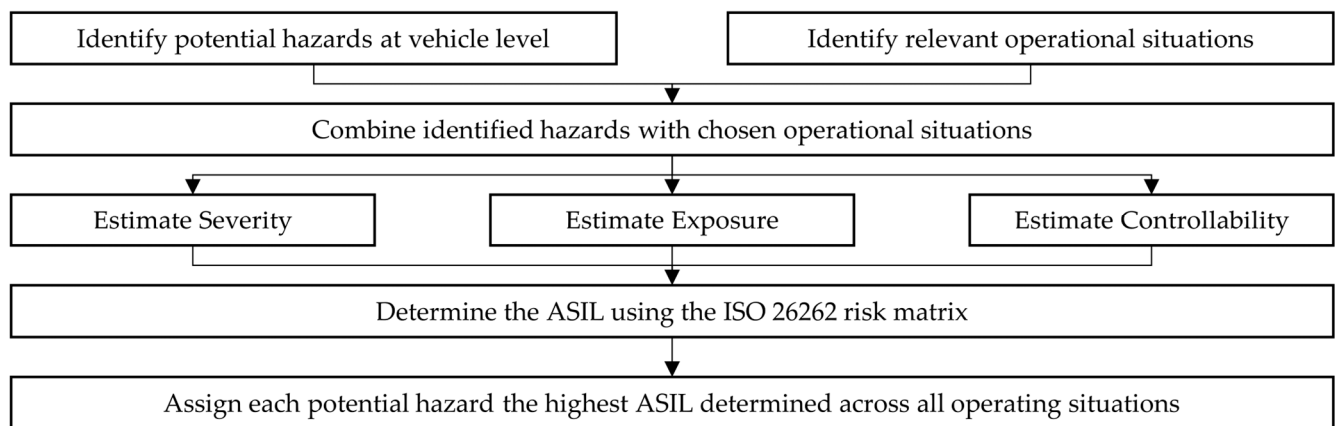


Figure 1. Schematic process of the HARA.

Hazards are defined as potential sources of harm caused by malfunctioning system behavior. Typical examples include vehicle motion hazards such as unintended vehicle acceleration due to excessive torque. In addition to qualitative descriptions, hazards can also be defined quantitatively, for example by specifying threshold-based criteria for unsafe behavior [14]. ISO 26262 lists structured methods such as Hazard and Operability Study (HAZOP) as suitable techniques to support hazard identification.

For each identified hazard, relevant operational situations are determined, describing scenarios that may occur during vehicle operation. Hazardous events are then defined as the combination of a hazard and an operational situation. Each hazardous event is evaluated in terms of Severity (S), Exposure (E), and Controllability (C), which represent the potential harm, the likelihood of occurrence, and the ability to avoid or mitigate the event, respectively. These factors are categorized into discrete classes, with Severity ranging from S0 to S3, Exposure from E0 to E4, and Controllability from C0 to C3. Based on these parameters, the ASIL is determined using the ISO 26262 risk matrix. The ASIL (A–D) defines the required rigor of subsequent safety measures, while QM indicates that standard quality processes are sufficient. If multiple operational situations result in different ASILs for the same hazard, the highest ASIL shall be assigned. Based on the resulting ASIL, safety goals are derived to define the top-level safety requirements for preventing or mitigating the corresponding hazardous events.

Manual HARA is inherently limited by a lack of objectivity, as key parameters are typically assessed qualitatively and depend strongly on individual expertise and judgment. As a result, different engineers may assign significantly different risk classifications for the same hazardous event. Approaches such as independent reassessment by a second team have been proposed to mitigate bias but remain resource-intensive and still show discrepancies in the results [15]. Empirical studies further highlight this variability. Both inexperienced and expert engineers exhibit inconsistencies in HARA outcomes, with expert assessments additionally influenced by experience-driven biases [16]. Rule-based approaches improve consistency, but ASIL classifications still vary across evaluators and are often application-specific [17].

2.2. Severity and Controllability Estimation Approaches for HARA

To support Severity assessment in HARA, ISO 26262: Part 3 (Annex B) recommends the use of medical injury severity classifications, such as the Abbreviated Injury Scale (AIS), Maximum AIS (MAIS), or Injury Severity Score (ISS). However, mapping specific driving scenarios to these scales still relies heavily on expert judgment. To improve consistency,

several studies use crash data to relate injury outcomes to collision characteristics for pedestrians and vehicle-to-vehicle accidents [18–22].

Quantitative approaches aim to estimate Severity based on measurable parameters, although this remains challenging due to interdependencies between influencing factors [2]. A common approach, also reflected in SAE J2980 [23], relates injury severity to the change in velocity of the vehicle during a collision, which serves as a key indicator of crash severity. This metric captures both vehicle dynamics and physical properties, is supported by statistical analyses of crash data [19,20,24], and is adopted in HARA approaches for Severity estimation [25]. Relative collision speed (closing speed) is widely applied as an indicator of collision Severity [22,26,27], while some simulation-based approaches incorporate collision impulse as a measure of momentum transfer [6,8]. In addition, absolute vehicle speed at impact is considered in [3], and, in certain cases, collision direction is included to refine Severity classification [7,21].

Controllability can be assessed using empirical data, simulation or vehicle tests, as well as expert judgment, as suggested in SAE J2980 [23]; in practice, this is typically realized through driving-simulator studies, real-world data, or reference examples provided in ISO 26262. Quantitative approaches estimate Controllability based on measurable parameters; however, the assessment remains challenging due to driver behavior variability and differences across use cases. Time-to-Collision and driver reaction time are commonly used as indicators to evaluate the available time for intervention [4,5,8,17,28]. In addition, vehicle dynamics parameters—including acceleration or deceleration and vehicle speed—are commonly considered to assess the ability to avoid or mitigate hazardous events [8,17]. Other approaches consider parameters such as distance to obstacles [17], as well as lateral deviation and yaw rate for specific maneuvers [6]. Furthermore, the Point-of-No-Return (PoNR) can be used as a criterion to define the boundary between controllable and uncontrollable situations [29].

2.3. Exposure Estimation of Combined Operational Situations

For Exposure assessment, ISO 26262 and VDA 702 provide guidance and representative examples [30]; however, these are limited to single-factor operational situations and do not address the evaluation of combined conditions. As a result, Exposure estimation for combined operational situations largely depends on engineering judgment, with limited guidance on handling dependencies between contributing factors.

Quantitative approaches based on probability estimation face significant challenges. While VDA 702 and SAE J2980 suggest combining probabilities under assumptions of independence, such assumptions are rarely valid in practice, as contributing factors are often correlated. Moreover, the required probabilistic data are typically unavailable, and simplistic combinations may lead to unrealistic or underestimated Exposure values [31,32]. Existing studies either rely on expert judgment for combined scenarios [33] or propose theoretical, data-intensive methods that are difficult to apply in practice [34,35]. Other works highlight the combinatorial complexity of systematically combining multiple factors and the associated data requirements, which limit applicability in real-world development [32,35].

3. Materials and Methods

This section presents the proposed simulation-based methodology for quantitative HARA of BEVs. The methodology consists of three main steps. First, combined operational situations are defined based on relevant contributing factors, such as initial vehicle speed, road surface, initial vehicle gap, road inclination, and collision type. Second, Severity and Controllability are evaluated using rule-based criteria, including a dedicated Controllability rule set for longitudinal motion hazards. Third, a bisection-based threshold search is

applied to derive quantitative erroneous acceleration and deceleration boundary values associated with different ASILs. Together, these steps enable a structured and reproducible assessment of longitudinal hazards across a broad range of operational situations.

3.1. Operational Situation Description

As stated in SAE J2980, an exhaustive analysis of all possible combinations of contributing factors is not required; instead, it is sufficient to consider representative operational situations, including those that lead to the highest ASIL. However, the decision regarding which operational situations are relevant for a particular hazard and which are likely to result in the highest ASIL is inherently subjective, susceptible to personal bias, and strongly dependent on the engineer's experience.

In this work, the exhaustive combination of contributing situational factors is adopted. To avoid the issues identified by Weitzel [31]—in particular the artificial limitation of the ASIL caused by multiplying low-probability situational factors—this study applies a lowest Exposure approach. For a set of contributing factors with individual Exposure ratings E_i , the Exposure of the combined operational situation is defined as the *lowest* Exposure rating among these factors, as shown in Equation (1).

$$E_{\text{Op.Sit.}} = \min(E_i) \quad (1)$$

The use of the lowest Exposure approach is based on interpreting combined operational situations as logical AND combinations. Since all conditions must occur simultaneously, the combined situation cannot be more frequent than the least frequent contributing factor. This approach is conservative with respect to a full probabilistic combination; for example, a combination of two independent E2 factors will still be classified as E2. However, it avoids the need to model complex statistical dependencies between situational parameters. Furthermore, the only required inputs for estimating Exposure in this method are the Exposure ratings of the contributing factors, which can be obtained from sources such as ISO 26262-3 or the VDA 702 situation catalogue. This makes the approach practical for real automotive applications where representative fleet data may not be available. Instead of debating probabilities and potential correlations between contributing factors, engineers can focus on assigning Exposure ratings, which is an inherently more manageable and transparent process. More advanced aggregation techniques, such as probabilistic combination [32] or fuzzy logic [36], could also be applied if suitable data or justified assumptions are available.

To enable simulation-based analysis, operational situations are represented quantitatively through parameters describing relevant contributing factors. Exposure classifications and corresponding parameter values—such as initial vehicle speed, road surface condition (dry, wet, snow) represented by friction coefficient, lighting conditions (daylight, darkness) reflected in driver reaction time, and road inclination (flat, moderate, steep)—are systematically derived in accordance with VDA 702. To account for collisions involving different types of road users (e.g., vehicles or pedestrians), distinct Severity mappings are applied. As no harmonized specification exists for quantifying inter-vehicle distance in HARA, the vehicle gap for Exposure class E4 is assumed to be proportional to vehicle speed and defined as the distance travelled within 2 s. Reduced gaps, representing tailgating as a form of reasonable misuse, are defined relative to this reference as 40% (E3) and 20% (E2).

It should be noted that choosing appropriate categories for relevant contributing factors is essential to avoid artificially lowering the Exposure. Splitting a contributing factor into overly specific subcategories or single values could lead to an unjustified reduction in Exposure, since a single value occurs less frequently than the broader category to which it belongs. Thus, contributing factors should be defined at a suitable level of abstraction.

3.2. Hazardous Event Analysis

Each operational situation, combined with a specific hazard (i.e., unintended acceleration or deceleration), defines a hazardous event that is simulated and evaluated with respect to Severity and Controllability. Fault injection is implemented by modifying the propulsion torque relative to the nominal operating point of the electric machine. The powertrain characteristics are considered such that the maximum available drive torque decreases with increasing vehicle speed. Vehicle resistances are accounted for, capturing environmental influences on vehicle dynamics.

Following fault injection, vehicle dynamics are simulated. For Severity estimation, a worst-case assumption is applied, neglecting driver reaction and thus leading to a collision with a preceding vehicle or pedestrian. As shown in Figure 2, maximum torque injection results in peak vehicle acceleration, which subsequently decreases with rising vehicle speed due to reduced available tractive force. For small torque deviations, the resulting acceleration is low, leading to a slow increase in vehicle speed and potentially long times to collision.

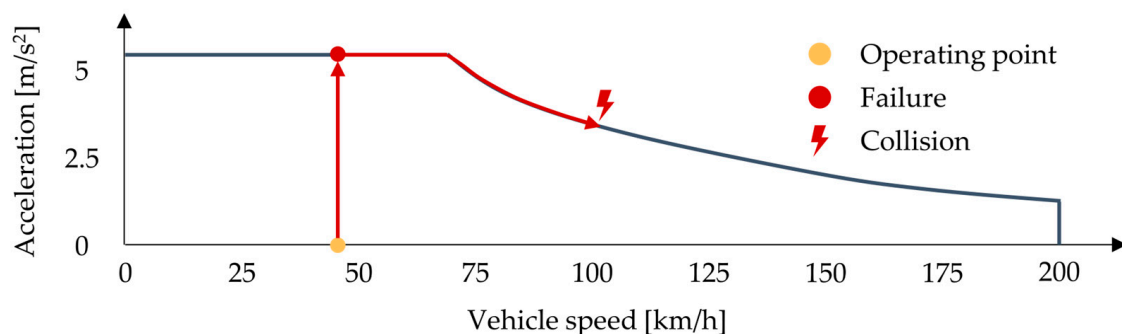


Figure 2. Unintended acceleration simulation for Severity estimation.

The collision speed is used to determine the Severity class of the hazardous event, as illustrated in Figure 3. Depending on the collision scenario—either a collision with a pedestrian or a rear-end collision with another vehicle—different Severity classification rules are applied. The threshold values are derived from informative examples in ISO 26262 [1] and statistical accident and injury data [18,19,21]. They represent one possible set of values and may be adapted or replaced based on alternative data sources.

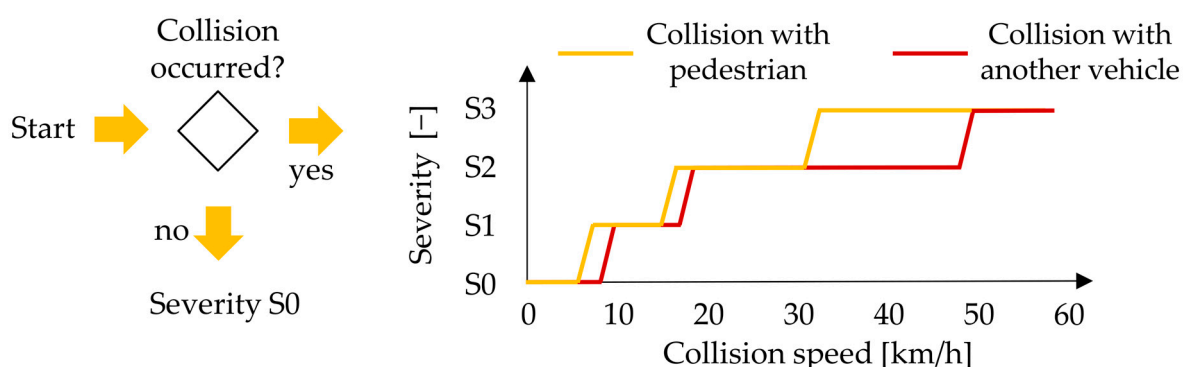


Figure 3. Severity estimation rule set.

A separate simulation is performed to determine the Controllability class. In this case, driver reaction is considered by assuming full braking after a defined delay following fault injection. It is important to distinguish between driver reactions to unintended deceleration and unintended acceleration, as they rely on different perception mechanisms. In the case of

unintended deceleration, the driver of the malfunctioning vehicle is generally unable to actively mitigate the hazard; instead, the response is required from the following driver, who reacts primarily based on visual perception of the preceding vehicle's behaviour (e.g., brake lights or decreasing distance) [37]. In contrast, for unintended acceleration, the response must be provided by the driver of the affected vehicle, who does not perceive the hazard visually but rather through vehicle motion, such as unexpected acceleration forces [38]. As illustrated in Figure 4, following fault injection, the vehicle speed initially increases during the driver's reaction time and then decreases once full braking is applied. The road surface condition, represented by the friction coefficient, determines the maximum braking force that can be transmitted to the road. Consequently, depending on the operational situation, the driver may or may not be able to avoid a collision.

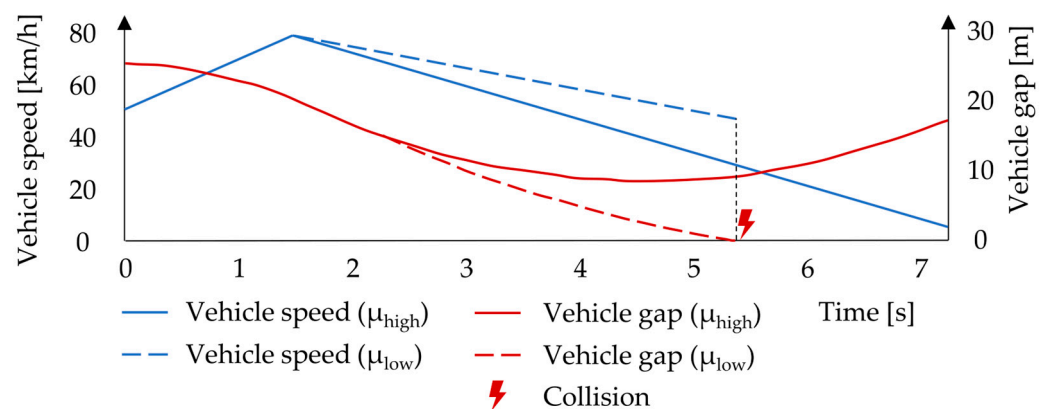


Figure 4. Unintended acceleration simulation for Controllability estimation.

ISO 26262 defines Controllability as the ability of the driver to regain sufficient control of a hazardous event to avoid harm. In this work, Controllability is evaluated based on whether a collision can be avoided by full braking while maintaining the intended driving path. If collision avoidance can be achieved through braking alone, controllability class C2 is assigned in accordance with ISO 26262-3, Annex B. If full braking is insufficient and additional steering is required to avoid the collision, the event corresponds to Controllability C3, as steering maneuvers represent a more demanding driver response. Figure 5 illustrates the rule set used for Controllability classification.

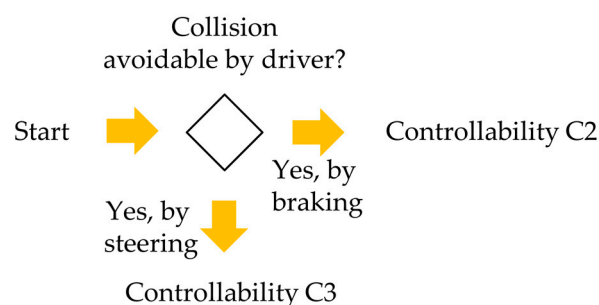


Figure 5. Controllability estimation rule set.

Alternative driver interventions, such as shifting to Neutral, are not considered for the Controllability estimation. While shifting to Neutral may be effective in vehicles with an internal combustion engine, where it can mechanically interrupt the power flow to the wheels, Neutral in BEVs is typically implemented as an electronic request within the propulsion control system. Therefore, its effectiveness cannot be assumed if the propulsion control path is already affected by the malfunction that caused the hazardous event.

A limitation of the proposed approach lies in the analysis of very low erroneous electric machine torques, which result in minor accelerations. The perception of such low-intensity unintended vehicle motions is difficult to describe within this modeling approach, as not all drivers may detect or correctly interpret these subtle deviations. Therefore, these cases are excluded from further analysis, as they are likely to correspond to lower Controllability classes.

3.3. Erroneous Acceleration Analysis

ASIL determination is commonly performed by assuming maximum fault magnitudes to evaluate worst-case conditions. However, it is also relevant to assess whether lower levels of erroneous torque result in comparable ASIL classifications. This enables a more detailed, quantitative characterization of hazards and supports subsequent verification of safety goals using measurable physical quantities, such as vehicle acceleration or deceleration.

For a given operational situation, the initial vehicle speed and initial vehicle gap are fixed, while the preceding vehicle maintains the initial speed. The velocity of the affected vehicle is calculated as follows:

$$v_{\text{ego}}(t) = v_0 + a_{\text{err}} * t. \quad (2)$$

The preceding vehicle maintains the initial velocity:

$$v_{\text{front}}(t) = v_0. \quad (3)$$

The resulting relative velocity is therefore expressed as follows:

$$v_{\text{rel}}(t) = v_{\text{ego}}(t) - v_{\text{front}}(t) = a_{\text{err}} * t. \quad (4)$$

The corresponding position of the affected vehicle is calculated:

$$s_{\text{ego}}(t) = v_0 * t + \frac{1}{2} * a_{\text{err}} * t^2. \quad (5)$$

For an initial vehicle gap d_0 , the preceding vehicle position is given by:

$$s_{\text{front}}(t) = d_0 + v_0 * t. \quad (6)$$

The remaining vehicle gap is obtained from the difference between the two positions:

$$d(t) = s_{\text{front}}(t) - s_{\text{ego}}(t) = d_0 - \frac{1}{2} * a_{\text{err}} * t^2. \quad (7)$$

A collision occurs when the remaining gap becomes zero:

$$t_{\text{col}} = \sqrt{\frac{2 * d_0}{a_{\text{err}}}}. \quad (8)$$

Accordingly, the relative collision speed is obtained by evaluating the relative velocity at the collision time:

$$v_{\text{col}} = a_{\text{err}} * t_{\text{col}} = \sqrt{2 * a_{\text{err}} * d_0}. \quad (9)$$

An increase in erroneous acceleration therefore results in a higher relative collision speed. Thus, Severity can be expressed as a nondecreasing function of the erroneous acceleration a_{err} :

$$a_{\text{err},1} < a_{\text{err},2} \Rightarrow v_{\text{col,err},1} < v_{\text{col,err},2} \Rightarrow S(a_{\text{err},1}) \leq S(a_{\text{err},2}). \quad (10)$$

Similarly, the Controllability is nondecreasing with increasing erroneous acceleration. In the simulation, the driver applies full braking after a fixed reaction time t_r . Provided that no collision occurs before the fixed reaction time t_r , the relative velocity at the beginning of braking is obtained:

$$v_{\text{rel},r} = a_{\text{err}} * t_r. \quad (11)$$

At the same time, the remaining vehicle gap is calculated:

$$d_r = d_0 - \frac{1}{2} * a_{\text{err}} * t_r^2. \quad (12)$$

Thus, increasing erroneous acceleration results in a higher relative velocity and a smaller remaining gap when the driver begins braking. Since the same full-braking intervention is applied for a fixed operational situation, these less favorable initial conditions reduce the possibility of avoiding the collision:

$$a_{\text{err},1} < a_{\text{err},2} \Rightarrow C(a_{\text{err},1}) \leq C(a_{\text{err},2}). \quad (13)$$

With a constant Exposure level for a given operational situation, the resulting ASIL classification is also nondecreasing with increasing erroneous acceleration.

$$a_{\text{err},1} < a_{\text{err},2} \Rightarrow ASIL(a_{\text{err},1}) \leq ASIL(a_{\text{err},2}). \quad (14)$$

The monotonicity of $S(a_{\text{err}})$, $C(a_{\text{err}})$, and $ASIL(a_{\text{err}})$ allows the determination of boundary values of erroneous acceleration at which the classification changes. For each ASIL q , the corresponding boundary is defined as the minimum erroneous acceleration that results in at least this ASIL:

$$a_{\text{err}}^{(q)} = \inf\{a_{\text{err}} \in [0, a_{\text{err,max}}] \mid ASIL(a_{\text{err}}) \geq q\}. \quad (15)$$

Since $ASIL(a_{\text{err}})$ is nondecreasing, the boundary values $a_{\text{err}}^{(q)}$ can be efficiently determined using a bisection search. The search starts with an interval $[a_{\text{low},0}, a_{\text{high},0}] = [0, a_{\text{err,max}}]$, where $a_{\text{low},k}$ denotes the lower bound (not reaching ASIL q) and $a_{\text{high},k}$ the upper bound (reaching or exceeding ASIL q) at iteration k .

In each iteration k , the midpoint is computed as

$$a_{\text{mid},k} = \frac{a_{\text{low},k} + a_{\text{high},k}}{2}. \quad (16)$$

If $ASIL(a_{\text{mid},k}) \geq q$, the upper bound is updated as $a_{\text{high},k+1} = a_{\text{mid},k}$; otherwise, the lower bound is updated as $a_{\text{low},k+1} = a_{\text{mid},k}$. This process is repeated until the interval width falls below a predefined tolerance of 0.05 m/s², yielding the boundary value $a_{\text{err}}^{(q)}$, which approximates the erroneous acceleration at which the ASIL classification changes.

As an example, Figure 6 presents the resulting boundaries for Severity (a), Controllability (b), and ASIL (c) for unintended acceleration, considering operational situations with varying initial vehicle speed, while all other parameters are fixed, namely a safe vehicle gap (E4), wet road surface (E3), no road inclination (E4), and vehicle-to-vehicle collision (E1–E4, depending on the initial vehicle speed). The boundary curves indicate the erroneous acceleration values at which a transition to a higher Severity class, Controllability class, or ASIL occurs.

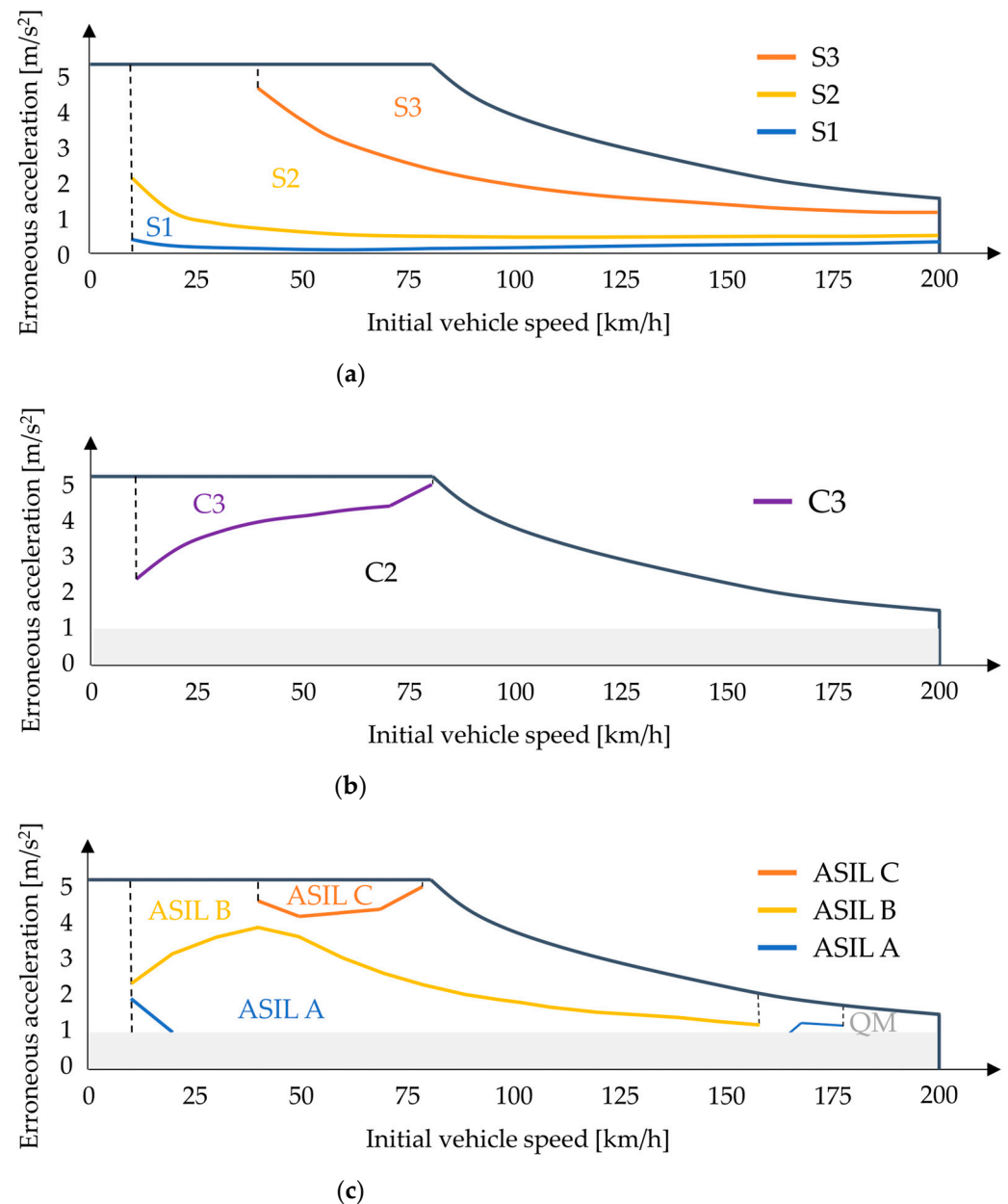


Figure 6. Severity (a), Controllability (b), and ASIL (c) boundaries for unintended acceleration as a function of initial vehicle speed, with fixed parameters (safe gap (E4), wet surface (E3), no slope (E4), vehicle-to-vehicle collision).

The decrease in Severity with increasing vehicle speed can be explained by the corresponding increase in vehicle gap, which is defined as proportional to vehicle speed. As a result, lower erroneous accelerations can lead to similar collision speeds. In contrast, Controllability decreases at lower vehicle speeds, as the driver has less time to react and avoid a collision through braking. The shaded region below an erroneous acceleration of 1 m/s^2 indicates a range that is excluded from the analysis, as Controllability cannot be reliably determined with the proposed approach. This limitation results from the underlying Controllability assessment method, which evaluates whether a collision can be avoided through full braking. However, such a driver reaction may not be appropriate for low-intensity unintended vehicle motions, as not all drivers may perceive or correctly interpret these subtle deviations. Consequently, a reliable assignment of Controllability classes cannot be ensured for these scenarios. The ASIL boundaries reflect the combined influence of the observed Severity and Controllability trends. In the considered operational

situations, the maximum Exposure is limited to E3 due to the wet road surface. At very high vehicle speeds, the resulting ASIL decreases as Exposure is further reduced (towards E2 and E1), leading to lower overall risk classifications.

Stationary situations, as shown in Figure 6, are excluded from the present analysis because they require different considerations regarding driver state and controllability. At a standstill, the driver may be outside the vehicle or seated in the vehicle but not attentive to the external environment, making the assessment of perception and reaction capability highly scenario-dependent. Such events are typically addressed under the separate hazard category of unintended propulsion from stationary [39] and are therefore considered outside the scope of this approach.

It is demonstrated that the torque–speed curve, which is determined by the available torque and power of the electric powertrain, is a decisive factor for the ASIL differences between vehicles with different performance capabilities. A reduction in the torque–speed curve leads to lower achievable acceleration values. As a result, the regions corresponding to higher Severity and Controllability classes, such as S3 and C3, become smaller or may no longer be reachable for a less powerful powertrain. This is also reflected in the resulting ASIL classification. In particular, Figure 6c shows that even a moderate change in powertrain performance can shift the resulting classification, for example, from ASIL C to ASIL B for the unintended acceleration hazard.

The same analysis can be applied to unintended deceleration by considering negative values of erroneous acceleration. In this case, a larger magnitude of deceleration results in stronger unintended braking, which correspondingly influences the resulting collision conditions and the derived Severity and Controllability classifications. In contrast to the analysis of unintended acceleration, the driver of the malfunctioning vehicle is not assumed to perform an additional reactive braking action, since the vehicle is already decelerating. Instead, the relevant avoidance action is attributed to the driver of the following vehicle, who may initiate braking once the abrupt deceleration of the preceding vehicle becomes perceptible. Since this reaction depends on visual perception of the preceding vehicle, visibility conditions may affect reaction time and thus the Controllability of the hazardous event. Therefore, lighting conditions, such as driving in daylight (E4) or at night without residual light (E3) according to VDA 702, can be considered contributing factors in combined operational situations.

4. Results

This section presents the application of the proposed simulation-based HARA methodology. First, the obtained results are compared with a manual HARA to identify agreement, as well as potential assessment biases and inconsistencies. Second, the simulation-based HARA results of two BEVs with different performance characteristics are compared and analysed. Finally, the methodology is applied to a Traffic Jam Assist function to demonstrate how the approach can support the definition of target ASILs for torque-determining vehicle functions. All simulation parameters and settings used in this study are provided in Appendix A.

4.1. Comparison Between Manual and Simulation-Based HARA

The proposed simulation-based approach was applied to the Tesla Model 3 [40], which features an electric powertrain with a single-speed transmission. A manually conducted HARA for light motor vehicles [39] served as a reference. The unintended acceleration hazard was selected to evaluate the approach.

Figure 7 shows the maximum Severity S, Controllability C, and ASIL for different operational situations at fixed initial vehicle speeds for vehicle-to-vehicle collisions. The

results show consistent trends in Severity and ASIL between both approaches, indicating that the simulation adequately reflects risk escalation with increasing speed. In contrast, Controllability differs: the manual HARA assigns C2 across all cases, whereas the simulation reveals speed-dependent variations, with Controllability decreasing toward C2 at higher speeds. This behavior can be explained by the characteristic torque map of the electric machine, which exhibits reduced torque at higher rotational speeds, thereby limiting unintended acceleration, as well as by typically smaller inter-vehicle distances at lower speeds, which reduce the available reaction time and thus decrease Controllability. Nevertheless, the results of the manual and simulation-based HARA are largely consistent. Both approaches also identify the same operational conditions leading to the highest ASIL, namely dry road conditions, medium to high initial vehicle speeds, and light traffic.

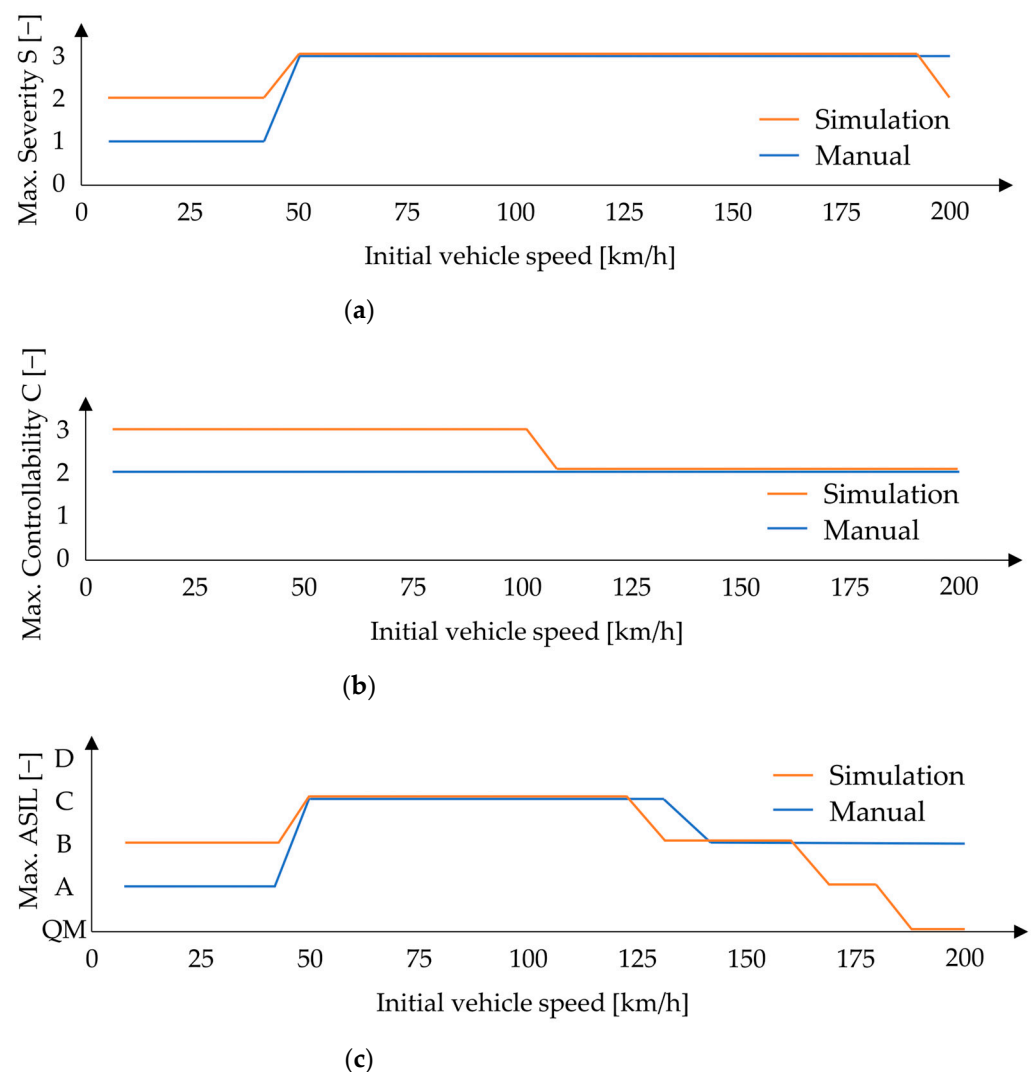


Figure 7. Maximum Severity (a), Controllability (b), and ASIL (c) as a function of initial vehicle speed (vehicle-to-vehicle collision).

To further deepen the analysis, a pairwise comparison of hazardous events was performed. Each hazardous event from the manual HARA was matched with its counterpart from the simulation-based HARA. The manual HARA contains fewer events due to aggregation of conditions (e.g., initial speed ranges), whereas the simulation evaluates discrete cases, resulting in multiple corresponding event pairs in such instances. For each pair, the resulting Severity, Controllability, and ASIL classifications from the manual and simulation-based HARA were compared. The results are presented in Figure 8. For each initial vehicle

speed, the figure indicates whether hazardous events are overestimated or underestimated by the manual HARA.

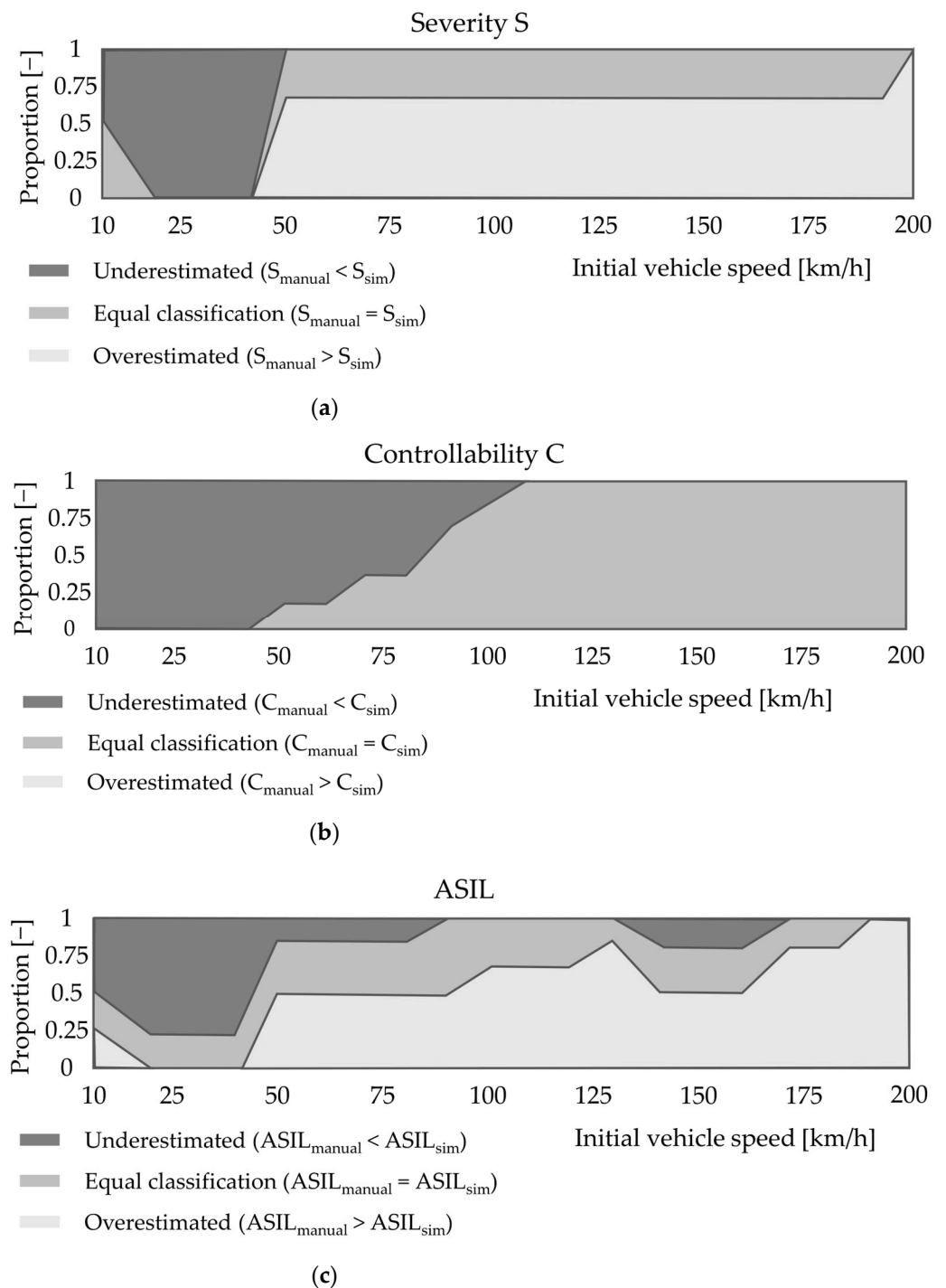


Figure 8. Proportion of Severity (a), Controllability (b), and ASIL (c) values overestimated or underestimated by the manually conducted HARA (vehicle-to-vehicle collisions).

Severity (a) is overestimated by the manual HARA at medium and higher speeds and underestimated at lower speeds. The manual HARA assigns Severity S3 for all situations above 40 km/h. However, in scenarios such as tailgating with short inter-vehicle distances, this may lead to overestimation, as the vehicle has limited time to further increase speed before impact. In addition, the characteristic torque map of the electric machine results in reduced acceleration at higher speeds, limiting the achievable impact velocity. At

lower speeds, the manual HARA assigns Severity S1, which may be appropriate for low-performance BEVs but can underestimate the risk for higher-performance vehicles, as reflected in the simulation results.

Regarding Controllability (b), the manual HARA assigns values between C1 and C2, whereas the simulation indicates a tendency toward C3, particularly at lower speeds. This is mainly due to smaller inter-vehicle distances, which reduce reaction time and may require simultaneous braking and steering. Furthermore, the manual HARA does not consider varying road conditions, assigning identical ratings regardless of surface friction, although reduced friction can further impact Controllability.

ASIL (c) is affected by both Severity and Controllability and therefore follows similar patterns. While maximum ASIL values are generally consistent between both approaches (Figure 7), deviations occur for less critical events. This highlights a limitation of the manual HARA, which captures worst-case classifications but provides less accuracy and consistency for intermediate scenarios compared to the simulation-based approach.

Furthermore, the results for vehicle-to-pedestrian collisions during unintended acceleration are shown in Figure 9. The analysis is limited by the low number of use cases. Nevertheless, both the simulation-based and manual HARA indicate ASIL B at very low speeds, mainly due to short distances to pedestrians, which prevent the vehicle from reaching critical collision speeds. At higher vehicle speeds, the simulation results indicate a higher ASIL, whereas the manual HARA shows no further increase in ASIL. This difference can be explained by different assumptions regarding collision avoidance by the pedestrians. In the automated approach, the ASIL classification is mainly driven by the higher impact velocity and the driver's ability to brake, while it is assumed that the pedestrian cannot avoid the collision by their own actions. In the manual HARA, however, lower Controllability classes are assigned, assuming that the pedestrian can evade the approaching vehicle.

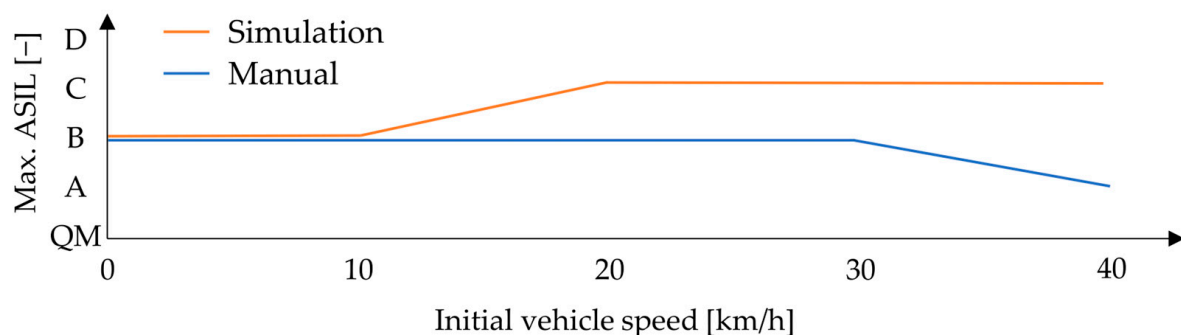


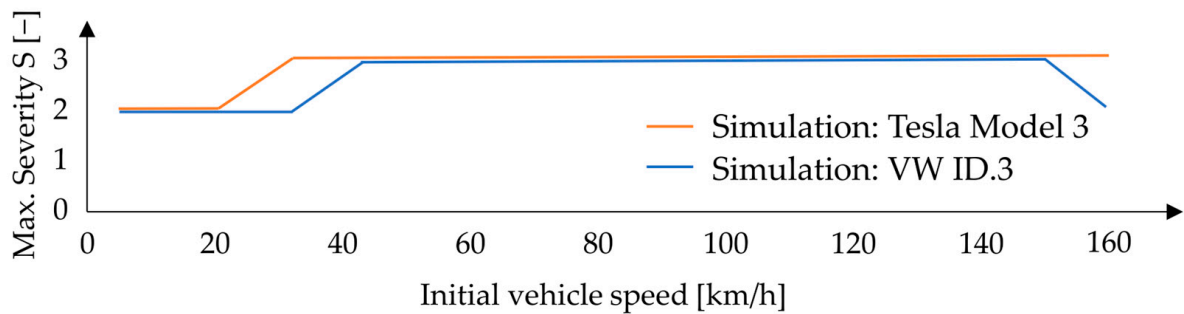
Figure 9. Maximum ASIL as a function of initial vehicle speed (vehicle-to-pedestrian collision).

4.2. Impact of Powertrain Performance on Simulation-Based HARA Results

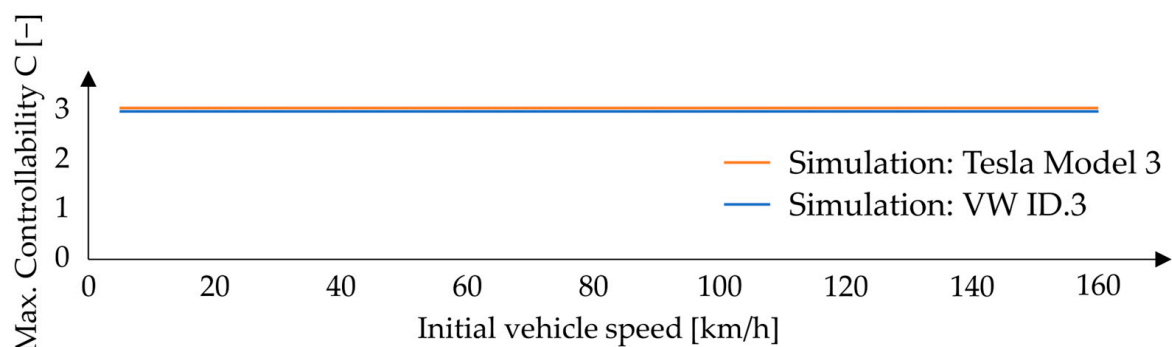
The proposed approach is suitable for ASIL determination across powertrains with different performance characteristics. To demonstrate this, the method was applied to two BEVs: the previously analysed Tesla Model 3 and the Volkswagen ID.3 [41]. Both vehicles employ electric powertrains with single-speed transmissions but differ in their maximum power and torque capabilities.

The results are shown in Figure 10, which presents the maximum Severity (a), Controllability (b), and ASIL (c) across all operational situations for each initial vehicle speed. A significant overlap in severity values is observed, and at least one hazardous event is classified with Controllability C3 for both vehicles. However, differences arise in ASIL: for vehicle-to-vehicle collisions, the less powerful Volkswagen ID.3 yields only ASIL B, whereas higher ASIL C is observed for the higher-performance Tesla Model 3. Exposure

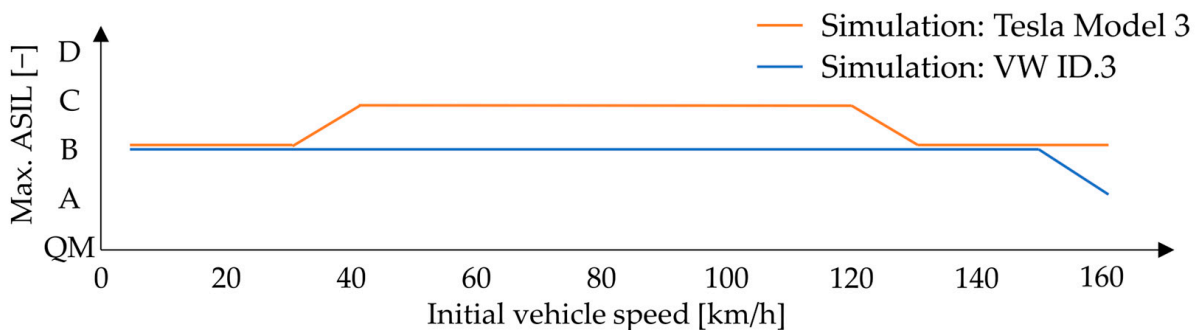
does not influence the ASIL difference, as the Exposure values for each operational situation are similar for both powertrains.



(a)



(b)



(c)

Figure 10. Maximum Severity (a), Controllability (b), and ASIL (c) as a function of initial vehicle speed (vehicle-to-vehicle collision) for simulative HARA of Tesla Model 3 and Volkswagen ID.3.

Figure 11 illustrates the reason for the different ASIL classifications of both powertrains, despite reaching the same maximum Severity and Controllability levels. For each combination of Severity and Controllability, the maximum Exposure and resulting ASIL across all corresponding hazardous events are shown. It can be observed that the combination of Severity S3 and Controllability C3 for the less powerful Volkswagen ID.3 occurs only in less frequent operational situations, such as low-friction road surfaces and negative inclines. In contrast, for the more powerful Tesla Model 3, higher Severity and Controllability levels are reached even in more common operational situations, leading to higher ASIL classifications.

		Controllability C [–]			
		C0	C1	C2	C3
Severity S [–]	S0				
	S1			E1 QM	E3 A
	S2			E3 A	E3 B
	S3			E4 C	E3 C

Tesla Model 3

(a)

		Controllability C [–]			
		C0	C1	C2	C3
Severity S [–]	S0				
	S1			E2 QM	E3 A
	S2			E4 B	E3 B
	S3			E3 B	E2 B

Volkswagen ID.3

(b)

Figure 11. Maximum Exposure and ASIL as a function of Severity and Controllability combinations for the Tesla Model 3 (a) and Volkswagen ID.3 (b).

Furthermore, results were obtained for vehicle-to-pedestrian collisions for both powertrains. These yielded similar outcomes, with ASIL C identified for both analysed vehicles; therefore, they are not discussed further.

In summary, this highlights the importance of considering vehicle-specific parameters when conducting a HARA. While the maximum ASIL for a given hazard may be identified by an experienced engineer with a strong understanding of the system, the interactions between powertrain characteristics and environmental conditions are difficult to assess in a structured manner. This may lead to inconsistencies in the analysis, which can be avoided by a simulation-based approach.

5. Use-Case Analysis

The proposed approach is applicable not only to the longitudinal hazard analysis of the overall powertrain, but also to individual torque-determining functions. In the vehicle, multiple torque requests may originate from different sources, including driver-initiated inputs (e.g., via the accelerator pedal), vehicle dynamics control functions (e.g., traction and stability control), and driver assistance functions (e.g., Adaptive Cruise Control, One Pedal Driving, Automatic Park Assist). These functions contribute differently to the overall vehicle behavior and may operate under restricted operational design domains (ODDs). Consequently, and with appropriate justification, certain functions can be developed to a lower ASIL than the overall powertrain due to their limited exposure and associated risk. A high-ASIL torque arbitration function is then required to safely coordinate, prioritize, and resolve competing torque requests, ensuring overall system safety.

To demonstrate the systematic definition of the ODD and associated constraints for achieving a target ASIL, a representative function is considered, namely Traffic Jam Assist (TJA). This function is implemented in various production vehicles [42,43] and may, depending on the use case, require a safety classification of up to ASIL D [44].

A conservative approach would assign the maximum ASIL derived at the powertrain level. For the unintended acceleration hazard in the Tesla Model 3 use case, this corresponds to ASIL C. However, due to the restricted ODD of TJA—typically limited to highway traffic conditions up to a predefined speed and characterized by a low probability of pedestrian presence—a lower ASIL classification may be justified. Furthermore, functional constraints, such as limiting the allowable acceleration, can be applied to reduce the associated risk.

To support this analysis, the proposed methodology evaluates combinations of operational situations, with selected examples shown in Figure 12. In each diagram, contributing factors—such as vehicle gap, road condition, and road inclination—are fixed, while the

initial vehicle speed is varied. For each case, the admissible ODD region is identified, indicating the conditions under which ASIL A can be achieved. Within this region, accelerations up to approximately 2.4 m/s^2 are permissible across all scenarios; higher accelerations may result in an ASIL B hazard in at least one case. Additionally, a speed limit of 50 km/h is derived for TJA operation, based on the assumption of Exposure class E4 at higher speeds. If a higher ASIL target (e.g., ASIL B) is acceptable, the ODD can be extended accordingly.

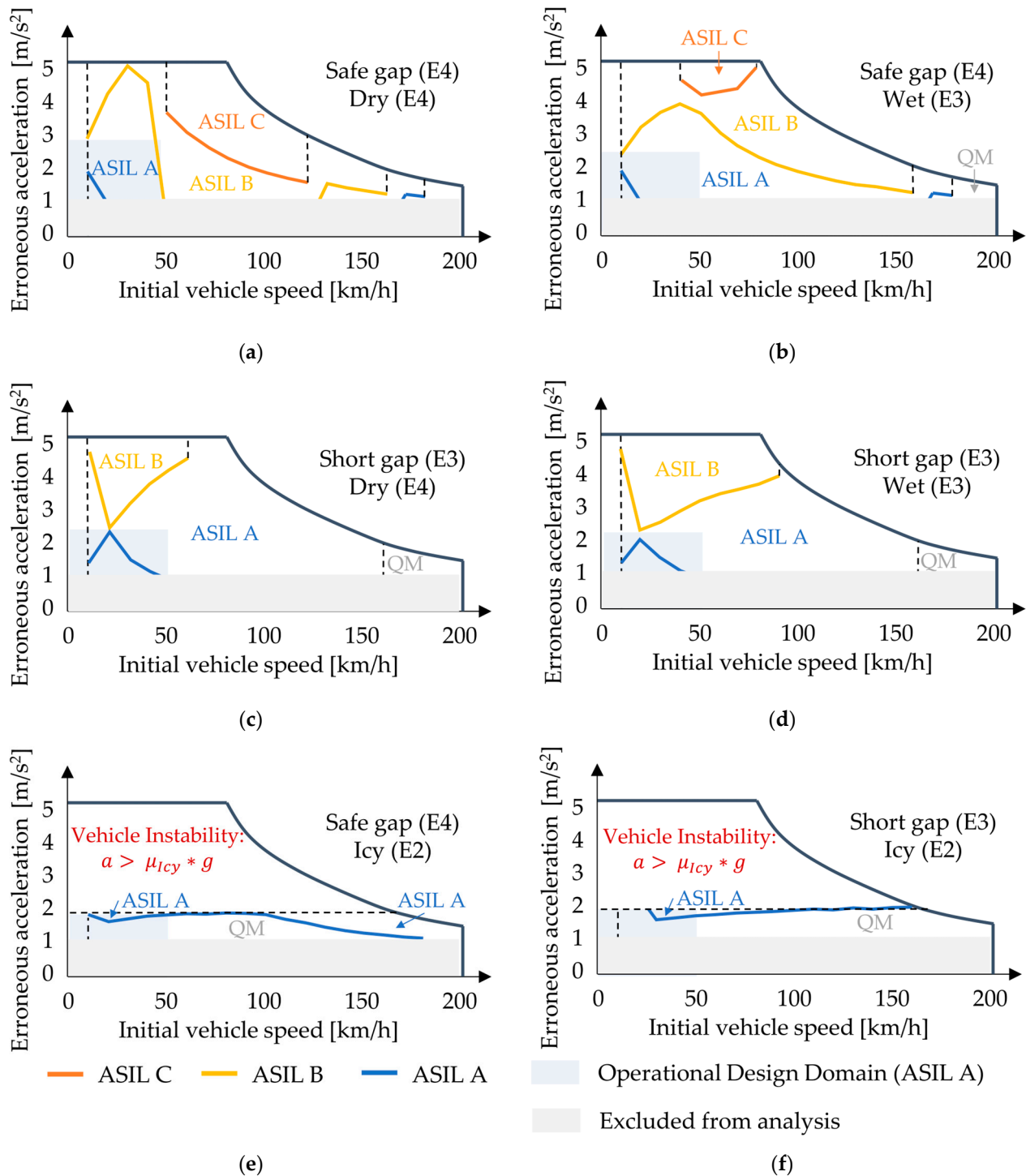


Figure 12. ASIL boundaries for unintended acceleration as a function of initial vehicle speed for vehicle-to-vehicle collision scenarios: (a) safe gap (E4), dry road (E4); (b) safe gap (E4), wet road (E3); (c) short gap (E3), dry road (E4); (d) short gap (E3), wet road (E3); (e) safe gap (E4), icy road (E2); and (f) short gap (E3), icy road (E2).

For low-friction surfaces, the tire-road adhesion limit must also be considered. The transferable longitudinal tire force is limited by the friction coefficient and the normal load; therefore, even relatively small unintended propulsion torques may lead to wheel slip on icy roads. This may subsequently affect lateral stability. In the present analysis, acceleration values that exceed the adhesion limit and lead to vehicle instability are excluded, since the focus is on longitudinal hazards. Stability-related hazards on low-friction surfaces are often associated with safety goals up to ASIL D [39] and should therefore be assessed in a dedicated analysis.

To address the unintended deceleration hazard of the TJA function, the same methodology is applied to negative electric machine torque across all relevant operational situations, including lighting conditions as an additional contributing factor. Selected examples are shown in Figure 13. The results indicate that, to remain within ASIL A, decelerations must be limited to approximately 1.7 m/s^2 . In addition, vehicle speed must not exceed 45 km/h , as higher speeds may result in higher ASIL even at these deceleration levels. If a higher ASIL target is acceptable, the ODD can be extended to allow both higher speeds and greater decelerations.

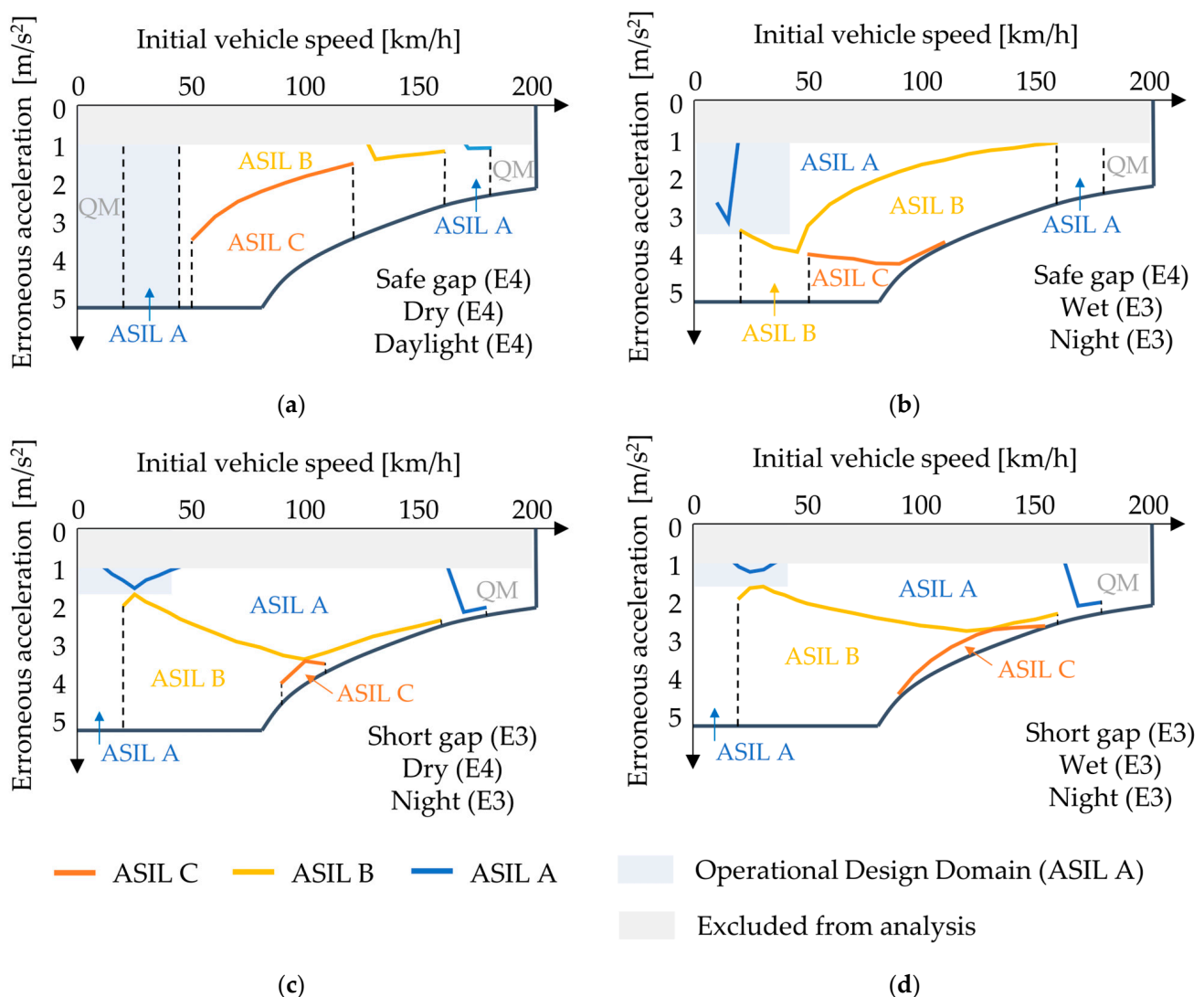


Figure 13. ASIL boundaries for unintended deceleration as a function of initial vehicle speed for vehicle-to-vehicle collision scenarios: (a) safe gap (E4), dry road (E4), and daylight conditions (E4); (b) safe gap (E4), wet road (E3), and nighttime conditions (E3); (c) short gap (E3), dry road (E4), and nighttime conditions (E3); and (d) short gap (E3), wet road (E3), and nighttime conditions (E3).

Overall, the methodology enables a systematic and transparent justification of ASIL allocation for vehicle functions. By evaluating all relevant operational situations, it identifies which conditions are admissible and which acceleration and deceleration limits ensure compliance with the target ASIL.

6. Discussion

In current practice, HARA is predominantly conducted manually, which limits objectivity and strongly depends on individual expertise. Furthermore, it is challenging for a human assessor to consistently evaluate how vehicle capabilities and specific hardware characteristics affect ASIL determination. This section presents the main biases and inconsistencies identified when comparing the manual HARA with the simulation-based HARA obtained using the developed approach. In addition, the integration of the approach into existing automotive safety workflows is discussed.

The first identified bias concerns notable variations in Controllability, which occur mainly at lower vehicle speeds. An engineer may intuitively assume that low-speed hazardous events are more controllable. However, at such speeds, vehicle gaps are usually also shorter, for example, in city traffic situations, which gives the driver less time to react. This represents a key finding of the rule-based simulation approach, as it shows that low vehicle speed does not inherently imply better Controllability of the hazardous event.

The second identified tendency concerns the underestimation of Severity by human assessors at low vehicle speeds. This is understandable, since higher vehicle speeds are intuitively associated with more severe collision outcomes, while lower speeds may be perceived as less dangerous. However, for BEV powertrains, maximum torque is typically available at low and medium vehicle speeds. As a result, unintended acceleration at low speeds can lead to a rapid increase in vehicle speed and therefore to higher collision speeds than may be expected intuitively. Conversely, the Severity of rear-end collisions at higher vehicle speeds may be overestimated. Due to the torque–speed characteristic of electric machines, less torque is typically available at higher speeds, which limits the achievable unintended acceleration.

Both identified biases also affect the resulting ASIL determination. The analysis shows that manual HARA for BEVs tends to underestimate ASIL at low vehicle speeds and overestimate it at medium to higher speeds.

Similar tendencies can be expected for vehicles with comparable powertrain performance and longitudinal dynamics, with the torque–speed curve being the main factor influencing the achieved ASIL. Since it determines the achievable acceleration, a less powerful powertrain may no longer reach acceleration levels associated with higher Severity or Controllability. This highlights the importance of considering vehicle-specific powertrain performance in HARA, rather than applying the same ASIL to all vehicle variants.

The proposed methodology can be used in the concept phase of powertrain development, as it requires only vehicle-level and operational-situation parameters that are typically available at this stage. It does not depend on a detailed electrical or control architecture of the vehicle. This also has a positive impact on computational effort, since only a longitudinal vehicle model and a bisection-based threshold search are used, rather than high-fidelity multidimensional vehicle or traffic simulations. Regarding accuracy, the method improves consistency and reproducibility compared with purely manual HARA. However, the results remain dependent on the selected assumptions, parameter values, and rule sets and should therefore be reviewed by experts. Finally, for validation of critical high-ASIL hazardous events or boundary cases, such as transitions between QM and ASIL-rated

classifications, high-fidelity simulation approaches can be applied in later development stages, when detailed system models are available.

Compared with previously published simulation-based HARA methods that mainly address lateral hazards, automated driving functions, or insufficient deceleration [3–5], the proposed approach systematically considers both unintended acceleration and unintended deceleration and determines quantitative erroneous acceleration and deceleration thresholds. In contrast to approaches restricted to highly exposed scenarios or conservative worst-case assumptions [6,7], it evaluates combined operational situations and varying fault magnitudes. Compared with methods requiring detailed vehicle models [8], the proposed approach uses a longitudinal vehicle model with fewer required parameters and is therefore more practical for application in early development stages.

This approach can be integrated into existing automotive safety workflows as a HARA support tool. It can be applied either during the initial HARA or later in the safety development process when additional hazardous events are identified. A relevant use case is the assessment of lower-ASIL hazardous events, which must also be analysed in HARA but usually receive less attention than highly critical cases. In this context, engineers can use their experience and judgment to identify the maximum ASIL, while the tool can support a more consistent assessment of lower-ASIL hazardous events. Furthermore, it may support functional safety audits by helping to check the consistency of the analysis. The typical engineering biases identified through the comparison with manual HARA may further serve as a basis for internal training or company workshops on consistent HARA creation.

However, the proposed methodology is intended to support HARA and improve consistency and traceability; it is not intended to replace expert review or established ISO 26262 safety lifecycle activities. The final classification should remain subject to expert judgment and appropriate safety justification.

7. Conclusions

This paper addressed the topic of HARA in functional safety for BEVs in accordance with ISO 26262. To address the limitations of manual HARA, a unified simulation-based approach was presented to support the analysis of longitudinal vehicle motion hazards. The proposed method combines multiple operational-situation parameters, such as vehicle speed, road surface, vehicle gap, road inclination, and collision type, to systematically evaluate their impact on Severity, Exposure, Controllability, and ASIL. This includes a dedicated Controllability rule set for longitudinal motion hazards. In addition to ASIL determination, the approach assesses different levels of unintended acceleration and deceleration and derives quantitative boundary values for safety goal violations using a bisection-based threshold search.

The results demonstrate that the proposed approach is a valuable complement to manual HARA. While the maximum ASIL for a given hazard can typically be identified based on engineering experience, the simulation-based approach improves consistency and coverage for lower-ASIL hazardous events. The comparison with manual HARA also revealed systematic assessment biases, showing at which initial vehicle speeds Severity, Controllability, and ASIL may be underestimated or overestimated by human assessors. Furthermore, the approach supports the evaluation of different powertrain variants by considering vehicle-specific performance characteristics, such as the torque–speed curve. The derived quantitative acceleration and deceleration limits can also support the development of torque-related vehicle functions by providing concrete targets for safety concept design, calibration, and validation.

In future work, the approach can be extended to additional longitudinal motion hazards and other electrified powertrains to further support quantitative HARA. In addition, the framework can be adapted to stationary use cases, such as unintended vehicle acceleration from standstill, which may require different assumptions regarding the driver's foot position and attention to the surrounding environment. Sensitivity analysis can be conducted to assess the influence of parameter variations on the resulting ASIL boundary values. Moreover, the methodology can be developed into a software-based framework to enable efficient and scalable application in industrial HARA processes. Finally, driving simulator studies, real-vehicle testing, or expert reviews should be conducted to validate the simulated Severity and Controllability boundary values and enable comparison with observed driver reactions and real vehicle behavior.

Author Contributions: Conceptualization, N.M.; methodology, N.M.; validation, N.M.; investigation, N.M.; resources, N.M.; data curation, N.M.; writing—original draft preparation, N.M.; writing—review and editing, S.P. and M.G.; visualization, N.M.; supervision, S.P. and M.G.; project administration, S.P. and M.G.; funding acquisition, N.M., S.P. and M.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
AIS	Abbreviated Injury Scale
ASIL	Automotive Safety Integrity Level
BEV	Battery Electric Vehicle
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard and Operability Study
ISO	International Organization for Standardization
ISS	Injury Severity Score
MAIS	Maximum Abbreviated Injury Scale
ODD	Operational Design Domain
PoNR	Point-of-No-Return
SAE	Society of Automotive Engineers
TJA	Traffic Jam Assist
QM	Quality Management

Appendix A

Appendix A.1

Table A1 summarizes the main simulation parameters used in the analysis. The table includes vehicle-related parameters for the Tesla Model 3 and Volkswagen ID.3, environmental parameters, and driver-related assumptions applied in the simulation-based HARA, enabling comparison between two BEVs with different performance characteristics.

Table A1. Summary of simulation parameters used in this study.

Parameter	Tesla Model 3	Volkswagen ID.3	Reference
Maximum torque [Nm]	420	350	[40,41]
Maximum power [kW]	239	150	[40,41]
Maximum engine speed [rpm]	16,000	16,000	[40,41]
Maximum vehicle speed [km/h]	225	160	[40,41]
Gear ratio [-]	9.04	11.53	[40,41]
Rotational inertia factor [-]	1.06	1.03	[40,41]
Vehicle mass [kg]	1825	1794	[40,41]
Driver + Passengers [kg]	150	150	[40,41]
Wheel radius [m]	0.3468	0.3468	[40,41]
Aerodynamic drag coefficient [-]	0.23	0.267	[45,46]
Frontal area [m ²]	2.22	2.36	[45,47]
Friction coefficient (dry) [-]		0.8	[30,48,49]
Friction coefficient (wet) [-]		0.5	[30,48,49]
Friction coefficient (snow/ice) [-]		0.2	[30,48,49]
Steep downhill road inclination		−0.10	[30]
Moderate downhill road inclination		−0.05	[30]
Flat road inclination		0	[30]
Moderate uphill road inclination		0.05	[30]
Steep uphill road inclination		0.10	[30]
Driver reaction time ¹ , daylight [s]		1.3	[37,50]
Driver reaction time ¹ , nighttime [s]		2.2	[51]
Affected-driver reaction time ² [s]		1.5	[38]

¹ Considered only for the unintended deceleration hazard. ² Considered only for the unintended acceleration hazard.

Appendix A.2

Table A2 summarizes the software environment, numerical solver configuration, and bisection stopping criterion used in the simulations.

Table A2. Simulation configuration of the proposed framework.

Parameter	Value/Setting
MATLAB/Simulink release	2025b
Numerical solver	Fixed-step discrete solver
Fixed-step size	0.025 s
Bisection algorithm stopping tolerance	0.05 m/s ²

Appendix A.3

Table A3 summarizes the operational-situation parameters and discrete states considered in this study. The operational-situation design space was generated by combining all applicable factor states. The selected states are specific to the present analysis and can be adapted for other applications.

Based on all applicable combinations of the contributing factors, 900 operational situations were simulated for the unintended acceleration hazard with the Tesla Model 3 and 720 with the Volkswagen ID.3. For the unintended deceleration hazard, including both visibility conditions, 1800 operational situations were simulated for the Tesla Model 3 and 1440 for the Volkswagen ID.3.

Table A3. Contributing factors used to define the operational-situation design space in this study.

Operational-Situation Parameter	States	Number of States
Road-surface condition	Low-, medium-, high-friction surfaces	3
Road inclination	Steep/moderate downhill, flat, moderate/steep uphill	5
Initial vehicle gap	20%, 40%, 100% of the safe distance ¹	3
Initial vehicle speed (Tesla Model 3)	10–200 km/h ²	20
Initial vehicle speed (VW ID.3)	10–160 km/h ²	16
Visibility condition ³	Daytime, nighttime	2

¹ Defined as the distance travelled within 2 s. ² In increments of 10 km/h. ³ Considered only for the unintended deceleration hazard.

References

- ISO 26262; Road Vehicles—Functional Safety. International Organization for Standardization ISO: Geneva, Switzerland, 2018.
- Ständer, T. Eine Modellbasierte Methode zur Objektivierung der Risikoanalyse Nach ISO 26262. Doctoral Dissertation, Universität Braunschweig, Braunschweig, Germany, 2010. [\[CrossRef\]](#)
- Ramic, A.; Kugele, S. Simulation-Based Support for Semi-Automated Automotive Safety Analysis. In *Proceedings of the IEEE 26th International Conference on Intelligent Transportation Systems (ITSC)*, Bilbao, Spain, 24–28 September 2023; IEEE: New York, NY, USA, 2023; pp. 1787–1794. [\[CrossRef\]](#)
- Sini, J.; Violante, M.; Dodde, V.; Gnani, R.; Pecorella, L. A Novel Simulation-Based Approach for ISO 26262 Hazard Analysis and Risk Assessment. In *Proceedings of the IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, Rhodes, Greece, 1–3 July 2019; IEEE: New York, NY, USA, 2019; pp. 253–254. [\[CrossRef\]](#)
- Sini, J.; Violante, M. A simulation-based methodology for aiding advanced driver assistance systems hazard analysis and risk assessment. *Microelectron. Reliab.* **2020**, *109*, 113661. [\[CrossRef\]](#)
- Barreto, J.; Rafael, A.; Bachir, Z. SAHARA: Simulation aided hazard analysis and risk assessment methodology. In *WIT Transactions on Engineering Sciences*; WIT Press: Southampton, UK, 2020; pp. 41–53. [\[CrossRef\]](#)
- Schrade, S.; Nowak, X.; Verhagen, A.; Schramm, D. Generic X-Domain Hazard Analysis and Risk Assessment. In *WCX SAE World Congress Experience*; SAE Technical Paper Series; SAE: Detroit, MI, USA, 2023. [\[CrossRef\]](#)
- Oakes, B.J.; Moradi, M.; van Mierlo, S.; Vangheluwe, H.; Denil, J. Machine Learning-Based Fault Injection for Hazard Analysis and Risk Assessment. In *Computer Safety, Reliability, and Security*; Springer: Cham, Switzerland, 2021; pp. 178–192. [\[CrossRef\]](#)
- Nouri, A.; Cabrero-Daniel, B.; Torner, F.; Sivencrona, H.; Berger, C. Welcome Your New AI Teammate: On Safety Analysis by Leashing Large Language Models. In *Proceedings of the IEEE/ACM 3rd International Conference on AI Engineering—Software Engineering for AI*; ACM: New York, NY, USA, 2024; pp. 172–177. [\[CrossRef\]](#)
- Hillen, D.; Helten, C.; Reich, J. Towards LLM-augmented Situation Space Analysis for the Hazard and Risk Assessment of Automotive Systems. In *INFORMATIK 2024*; Gesellschaft für Informatik e.V.: Bonn, Germany, 2024. [\[CrossRef\]](#) [\[PubMed\]](#)
- Sabbella, R.R.; Arunachalam, M. Functional Safety Development of Motor Control Unit for Electric Vehicles. In *Proceedings of the IEEE Transportation Electrification Conference (ITEC-India)*; IEEE: New York, NY, USA, 2019; pp. 1–6. [\[CrossRef\]](#)
- Bhavana, R.; Indela, O.; Yaragatti, M.S. Functional safety requirements of traction inverter in accordance to ISO 26262. *E3S Web Conf.* **2020**, *184*, 1062. [\[CrossRef\]](#)
- Ertas, I.C.; Özçira Özkılıç, S.; Dalkılıç, Ç.; Soygenç, O.C. A Case Study: Inverter Safety in Compliance with ISO26262. In *Proceedings of the 14th International Conference on Electrical and Electronics Engineering (ELECO)*, 30 November–2 December 2023; IEEE: New York, NY, USA, 2023; pp. 1–5. [\[CrossRef\]](#)
- Suerken, M.; Peikenkamp, T. Model-based Application of ISO 26262: The Hazard Analysis and Risk Assessment. *SAE Int. J. Passeng. Cars—Electron. Electr. Syst.* **2013**, *6*, 114–125. [\[CrossRef\]](#)
- Veland, H.; Aven, T. Improving the risk assessments of critical operations to better reflect uncertainties and the unforeseen. *Saf. Sci.* **2015**, *79*, 206–212. [\[CrossRef\]](#)
- Beckers, K.; Holling, D.; Côté, I.; Hatebur, D. A structured hazard analysis and risk assessment method for automotive systems—A descriptive study. *Reliab. Eng. Syst. Saf.* **2017**, *158*, 185–195. [\[CrossRef\]](#)
- Khastgir, S.; Birrell, S.; Dhadyalla, G.; Sivencrona, H.; Jennings, P. Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems. *Saf. Sci.* **2017**, *99*, 166–177. [\[CrossRef\]](#)
- Tefft, B.C. Impact speed and a pedestrian's risk of severe injury or death. Accident; analysis and prevention. *Accid. Anal. Prev.* **2013**, *50*, 871–878. [\[CrossRef\]](#) [\[PubMed\]](#)

19. Richards, D.C. *Relationship Between Speed and Risk of Fatal Injury: Pedestrians and Car Occupants*; Department for Transport: London, UK, 2010.
20. Verma, M.K.; Goertz, A. Preliminary Evaluation of Pre-Crash Safety System Effectiveness. In *SAE 2010 World Congress & Exhibition*; SAE Technical Paper Series; SAE: Warrendale, PA, USA, 2010. [CrossRef]
21. Jurewicz, C.; Sobhani, A.; Woolley, J.; Dutschke, J.; Corben, B. Exploration of Vehicle Impact Speed—Injury Severity Relationships for Application in Safer Road Design. *Transp. Res. Procedia* **2016**, *14*, 4247–4256. [CrossRef]
22. Lubbe, N.; Wu, Y.; Jeppsson, H. Safe speeds: Fatality and injury risks of pedestrians, cyclists, motorcyclists, and car drivers impacting the front of another passenger car as a function of closing speed and age. *Traffic Saf. Res.* **2022**, *2*, 000006. [CrossRef]
23. SAE J2980; Considerations for ISO 26262 ASIL Hazard Classification. SAE International: Warrendale, PA, USA, 2015. [CrossRef] [PubMed]
24. Wang, J.-S. *MAIS(05/08) Injury Probability Curves as Functions of Delta V (Report No. DOT HS 813 219)*; National Highway Traffic Safety Administration: Washington, DC, USA, 2022.
25. Duracz, A.; Eriksson, H.; Bartha, F.A.; Xu, F.; Zeng, Y.; Taha, W. Using Rigorous Simulation to Support ISO 26262 Hazard Analysis and Risk Assessment. In *Proceedings of the IEEE 17th International Conference on High Performance Computing and Communications, 24–26 August 2015*; IEEE: New York, NY, USA, 2015; pp. 1093–1096. [CrossRef]
26. Doecke, S.D.; Baldock, M.R.J.; Kloeden, C.N.; Dutschke, J.K. Impact speed and the risk of serious injury in vehicle crashes. *Accid. Anal. Prev.* **2020**, *144*, 105629. [CrossRef] [PubMed]
27. Krampe, J.; Junge, M. Injury Severity for Hazard & Risk Analyses: Calculation of ISO 26262 S-parameter Values from Real-World Crash Data. *Accid. Anal. Prev.* **2020**, *138*, 105321. [CrossRef] [PubMed]
28. Liu, R.; Lu, K.; Zhu, Y.; Wu, Z. An Evaluation Method of Vehicle Functional Safety Controllability Based on Driver-in-the-Loop Platform. *J. Phys.* **2022**, *2173*, 012054. [CrossRef]
29. Weitzel, D.A. Objektive Bewertung der Kontrollierbarkeit Nicht Situationsgerechter Reaktionen Umfeldsensorbasierter Fahrerassistenzsysteme. Doctoral Dissertation, Darmstadt University of Technology, Darmstadt, Germany, 2013. [CrossRef]
30. Verband der Automobilindustrie. *VDA 702: Situationskatalog E-Parameter Nach ISO 26262-3*; Verband der Automobilindustrie e.V.: Berlin, Germany, 2015.
31. Weitzel, A.; Winner, H. *Controllability Assessment for Unintended Reactions of Active Safety Systems*; National Academies: Washington, DC, USA, 2013. Available online: <https://trid.trb.org/View/1360434> (accessed on 1 April 2026).
32. Nag, P.; Harmalkar, J.; Ghanekar, U. A Novel Hazard Analysis and Risk Assessment for Automotive Embedded System Development as Safety Element Out of Context. In *Proceedings of the 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*; IEEE: New York, NY, USA, 2019; pp. 664–669. [CrossRef]
33. Czerny, B.J.; Suchala, R.; Runyon, M. A Scenario-Based Approach to Assess Exposure for ASIL Determination. In *SAE 2014 World Congress & Exhibition*; SAE Technical Paper Series; SAE: Warrendale, PA, USA, 2014. [CrossRef]
34. Jang, H.A.; Kwon, H.M.; Hong, S.-H.; Lee, M.K. A Study on Situation Analysis for ASIL Determination. *J. Ind. Intell. Inf.* **2014**, *3*, 152–157. [CrossRef]
35. Kemmann, S.; Trapp, M. SAHARA -A Systematic Approach for Hazard Analysis and Risk Assessment. In *SAE 2011 World Congress & Exhibition*; SAE Technical Paper Series; SAE: Warrendale, PA, USA, 2011. [CrossRef]
36. Merola, F.; Bernardeschi, C.; Lami, G. A Risk Assessment Framework Based on Fuzzy Logic for Automotive Systems. *Safety* **2024**, *10*, 41. [CrossRef]
37. Triggs, T.J.; Harris, W.G. *Reaction Time of Drivers to Road Stimuli*; National Academies: Washington, DC, USA, 1892.
38. Tao, C. Functional safety concept design of hybrid electric vehicle following ISO 26262. In *Proceedings of the IEEE Conference and Expo Transportation Electrification Asia-Pacific*; IEEE: New York, NY, USA, 2014; pp. 1–6. [CrossRef]
39. Becker, C.; Nasser, A.; Attioui, F. *Functional Safety Assessment of a Generic Accelerator Control System with Electronic Throttle Control in Electric Vehicles*; DOT HS 812 656; National Highway Traffic Safety Administration: Washington, DC, USA, 2020.
40. Rosenberger, N.; Rosner, P.; Bilfinger, P.; Schöberl, J.; Teichert, O.; Schneider, J. Quantifying the State of the Art of Electric Powertrains in Battery Electric Vehicles: Comprehensive Analysis of the Tesla Model 3 on the Vehicle Level. *World Electr. Veh. J.* **2024**, *15*, 268. [CrossRef]
41. Wassiliadis, N.; Steinsträter, M.; Schreiber, M.; Rosner, P.; Nicoletti, L.; Schmid, F. Quantifying the state of the art of electric powertrains in battery electric vehicles: Range, efficiency, and lifetime from component to system level of the Volkswagen ID.3. *eTransportation* **2022**, *12*, 100167. [CrossRef]
42. Audi. Audi AI Traffic Jam Pilot. Available online: <https://magazine.audi.com.au/article/audi-ai-traffic-jam-pilot> (accessed on 7 April 2026).
43. Mercedes-Benz. Mercedes-Benz DRIVE PILOT: The Front Runner in Automated Driving and Safety Technologies. Available online: <https://group.mercedes-benz.com/technology/autonomous-driving/driving/drive-pilot.html> (accessed on 7 April 2026).

44. He, L.; Ye, F.; Chen, J.; Li, H.; Di, Z. Research on Longitudinal Functional Safety Analysis of Traffic Jam Assist System. In *Proceedings of the 7th CAA International Conference on Vehicular Control and Intelligence (CVCI)*; IEEE: New York, NY, USA, 2023; pp. 1–4. [CrossRef]
45. Volkswagen of America, Inc. Newspress Limited, World Premiere of the Fully Electric ID.3: The First ID. Family Vehicle Debuts for the European Market. Available online: <https://media.vw.com/releases/1198> (accessed on 27 June 2026).
46. EVspecs.org. Tesla Model 3 RWD (2017-2023) Tech Specs. Available online: <https://www.evspecs.org/tech-specs/tesla/model-3-2017-2023/rwd> (accessed on 27 June 2026).
47. TheDriven.io. EV Range on Australian Highways: Why Model 3 Beats All Other Electric Cars on Efficiency. Available online: <https://thedriven.io/2023/09/07/ev-range-on-australian-highways-why-model-3-beats-all-other-electric-cars-on-efficiency/> (accessed on 27 June 2026).
48. Singh, K.B.; Taheri, S. Estimation of tire–road friction coefficient and its application in chassis control systems. *Syst. Sci. Control Eng.* **2014**, *3*, 39–61. [CrossRef]
49. Warner, C.Y.; Smith, C.C.; James, M.B.; Germane, G.J. Friction Applications in Accident Reconstruction. In *SAE International Congress and Exposition*; SAE Technical Paper Series; SAE: Warrendale, PA, USA, 1983. [CrossRef] [PubMed]
50. Green, M. “How Long Does It Take to Stop?” Methodological Analysis of Driver Perception-Brake Times. *Transp. Hum. Factors* **2000**, *2*, 195–216. [CrossRef] [PubMed]
51. Fotios, S.; Cheal, C.; Fox, S.; Uttley, J. The effect of fog on detection of driving hazards after dark. *Light. Res. Technol.* **2017**, *50*, 1024–1044. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.