

Article

Minimum Risk Maneuver Strategy for Automated Driving System Under Multiple Conditions of Sensor Failure

Junjie Tang, Chengxin Yang and Hidekazu Nishimura * 

Graduate School of System Design and Management, Keio University, Kanagawa 223-8526, Japan; tousyunnketu@keio.jp (J.T.); yangchengxin@keio.jp (C.Y.)

* Correspondence: nism@keio.jp

Abstract

To ensure the safety of vehicles and occupants under failures or functional limitations of ego vehicles, a minimum risk maneuver (MRM) has been proposed as a key automated driving system (ADS) function. However, executing an MRM may pose certain potential risks when sensor failures occur. This study proposed an MRM strategy designed to enhance highway-driving safety during MRM execution under multiple sensor-failure conditions. A hazard and operability study analysis, based on an ADS behavior model, is conducted to systematically identify hazards, determine potential hazardous events, and categorize the associated safety risks arising from sensor failures. Within the proposed strategy, virtual objects are generated to account for potential hazards and support risk assessments. Adaptive MRM behavior is determined in real time by analyzing surrounding objects and evaluating time-to-collision and time headway. The strategy is verified by using a MATLAB–CARLA co-simulation environment across three representative highway scenarios with combined sensor failures. The result demonstrates that the proposed MRM strategy can mitigate collision risk in hazardous scenarios while effectively leveraging the remaining functional sensors to guide the ego vehicle toward an appropriate minimum risk condition during MRM execution.

Keywords: automated driving system; minimum risk maneuver; vehicle safety; hazard and operability study; sensor failure; model-based systems engineering

1. Introduction

1.1. Background

Automated driving systems (ADSs) are among the most transformative innovations in modern transportation, with the potential to reduce traffic accidents, improve road efficiency, and enhance user comfort. According to the SAE J3016 taxonomy, automated driving levels range from 0 (no automation) to 5 (full automation). An ADS is defined as a system capable of performing the entire dynamic driving task (DDT) on a sustained basis, applicable to Levels 3 (conditional automation) to 5 only within a predefined operational design domain (ODD) [1].

At Level 4 and Level 5, the ADS is solely responsible for initiating a minimum risk maneuver (MRM) to bring the vehicle to a safe state when it can no longer operate safely. For a Level 3 ADS, although a driver is expected to respond to a takeover request, the ADS must also be capable of executing an MRM if the driver fails to respond [1–6].

The concept of an MRM is central to safe fallback strategies for ADSs. SAE J3016 defines a minimum risk condition (MRC) as a “stable, stopped condition” but does not



Academic Editors: Davide Shingo Usami and Brayan González-Hernández

Received: 18 November 2025

Revised: 4 January 2026

Accepted: 6 January 2026

Published: 13 January 2026

Copyright: © 2026 by the authors. 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.

explicitly define MRM, instead implying its necessity through the fallback process [1]. Additional guidance on fallback behavior appears in ISO 26262 [2], the Safety First for Automated Driving (SFFAD) white paper [3], the UN-ECE regulation on Automated Lane-keeping Systems (ALKS) [4], and EU Implementing Regulation (EU) 2022/1426 [5]. ISO 26262 does not use the term “MRM,” but it describes transitions to safe states under system failures. SFFAD introduces categories such as safe stop and emergency stop, broadening the MRC concept beyond a full halt to include transitional or operator-assisted states. To address degraded situations explicitly, the UN-ECE ALKS regulation introduces an emergency MRM, which requires bringing the vehicle to a controlled stop in its current lane, with deceleration up to or exceeding 4 m/s^2 when necessary for safety. EU Implementing Regulation (EU) 2022/1426 states that when failures affect braking or steering performance, an MRM should be executed with consideration of the remaining vehicle performance [5].

ISO 23793-1:2024 [6] provides one of the most comprehensive formal definitions of an MRM, describing it as a “coordinated combination of lateral and longitudinal driving actions executed by an ADS under degraded conditions.” The standard distinguishes MRMs from emergency braking or comfort stops by requiring them to be repeatable, verifiable, and interoperable. It classifies MRMs into three types:

- Type 1: Straight Stop (longitudinal deceleration only);
- Type 2: In-lane Stop (combined longitudinal and lateral control);
- Type 3: Road-shoulder Stop (lane change to exit traffic).

To simplify decision-making under degraded conditions, MRM selection is designed to follow a conservative sequence (e.g., preferring Type 3 before Type 2), generally avoiding transitions to more complex maneuvers. This structured approach underscores MRM as not merely a reactive safety measure but a context-aware, standards-compliant function critical to fail-operational ADS design.

Overall, existing standards provide an essential foundation for defining the roles and requirements of MRMs, yet they leave substantial room for implementation-level design and adaptive control strategies. This gap becomes particularly critical under sensor failures, where MRM execution must rely on uncertain perception and the effective use of remaining functional sensors. This motivates the need for a MRM strategy that explicitly accounts for multi-sensor failure scenarios, perception blind areas, and conservative safety decision-making during highway driving.

1.2. Previous Research

While existing standards provide high-level definitions and classifications of an MRM, their practical implementation remains an active research area.

Gyllenhammar et al. [7] proposed a theoretical safety framework that reinterprets the MRC as a strategic decision in a Level 4 ADS, introducing hierarchical MRC levels based on the environmental context and temporal constraints. Balakrishnan [8] developed a Level 3-oriented MRM implementation framework, distinguishing between normal and emergency MRMs and integrating functional safety concepts, hazard analysis, subsystem redundancy, and validation mechanisms.

Human–machine interface (HMI) design has also been investigated to support MRM communication. Schindler et al. [9] and Karakaya et al. [10] demonstrated that both external HMI (eHMI) and driver-focused HMI (dHMI)—such as directional lights and head-up displays—can enhance situational awareness and reduce driver response times. Nagayoshi et al. [11] and Hub et al. [12] further showed that synchronized audiovisual alerts and cooperative intent signaling improve the safety and predictability of MRMs in mixed-traffic scenarios.

Regarding motion planning, Tong et al. [13] proposed a unified planner capable of handling both nominal driving and MRM using search-based strategies and hybrid trajectory generation. Vu et al. [14] extended this approach to multi-agent scenarios, introducing global vs. local MRCs and collaborative MRMs to enable coordinated vehicle responses.

Additional studies have focused on fallback strategies aligned with MRM safety objectives. Svensson et al. [15] formulated the safe-stop problem as an optimal control task and proposed a trajectory-library approach supported by a safety monitor. Xue et al. [16] addressed sensor failures by introducing a virtual lead vehicle and model-predictive control for safe deceleration and lane changes. Wang et al. [17] developed a real-time trajectory planner combining a hybrid A* algorithm with space–time velocity optimization to manage both static and dynamic obstacles.

1.3. Gaps and Challenges

Despite growing research on MRM motion planning and decision-making, the impact of degraded perception due to sensor failures remains underexplored. In particular, few studies address how MRM strategies should adapt under partial sensor loss or uncertain environmental perception.

Xue et al. [16] proposed a fallback strategy for front-sensor failure using a virtual lead vehicle, but their model assumes fully functional side and rear sensors and does not account for broader or dynamic sensor failure. Similarly, Vu et al. [14] considered sensor failure through cooperative MRMs supported by surrounding autonomous vehicles, yet their approach relies heavily on vehicle-to-vehicle communication and precise localization, which may be infeasible in degraded infrastructure scenarios.

These gaps highlight two critical research challenges:

1. Systematically investigating how different types and locations of sensor failures affect MRM behavior and the associated safety risks;
2. Developing decision-making strategies that optimize MRM execution while accounting for risks arising from sensor failures and the dynamic safety conditions of the surrounding environment.

1.4. Objectives and Contributions

To address the identified research gaps, this study proposes an MRM strategy for Level 3 and Level 4 ADSs in highway-driving scenarios to enhance system safety. The strategy is designed to mitigate the risk of hazardous events during MRM execution, particularly under various sensor-failure conditions, thereby improving the safety of both the ego vehicle and its surrounding environment.

This study makes the following key contributions to advancing MRM for ADS under sensor-failure conditions:

1. A systematic hazard identification and classification for MRM execution under sensor failures.
The study identifies hazards and potential hazardous events that may arise during MRM execution under various sensor-failure conditions and systematically categorizes them into distinct hazard types.
2. An adaptive MRM decision strategy that effectively leverages remaining functional sensors under multiple sensor-failure scenarios.
The proposed strategy addresses the challenge of optimal MRM decision-making under multiple sensor-failure scenarios by enabling context-aware decisions based on perceptual information using the remaining functional sensors, thereby enhancing safety for both the ego vehicle and surrounding traffic participants.

Together, these contributions provide a practical and extensible methodology for enabling resilient MRM execution in real-world highway deployments of Level 3 and Level 4 ADSs.

In Section 2, a hazard and operability study (HAZOP) analysis is performed on a behavior model of the ADS to evaluate the impact of sensor failures. This analysis identifies relevant hazards and potential hazardous events and systematically assesses the associated risks related to MRM behavior.

Section 3 presents the complete proposed MRM strategy, including a perception compensation method tailored to sensor-failure conditions and adaptive decision-making for MRM behavior based on time-to-collision (TTC), time headway (THW), and current sensor status.

In Section 4, the proposed strategy is validated through simulations under three sensor-failure scenarios, demonstrating its feasibility and safety benefits.

2. HAZOP Analysis of Sensor Failure on MRM Behavior

2.1. ADS Behavior Model

To analyze the impact of various sensor-failure conditions on MRM execution, this study constructs a behavior model of the ADS task “Perform the DDT on highway” using the Systems Modeling Language (SysML) with CATIA Magic Systems of Systems Architect 2024x Refresh2, as illustrated in Figure 1 [18,19]. In SysML, an activity formally describes behavior by specifying the transformation of inputs into outputs through a controlled sequence of actions. The activity diagram provides the primary representation for modeling flow-based behavior and is analogous to the functional flow diagrams commonly used in systems engineering [20,21].

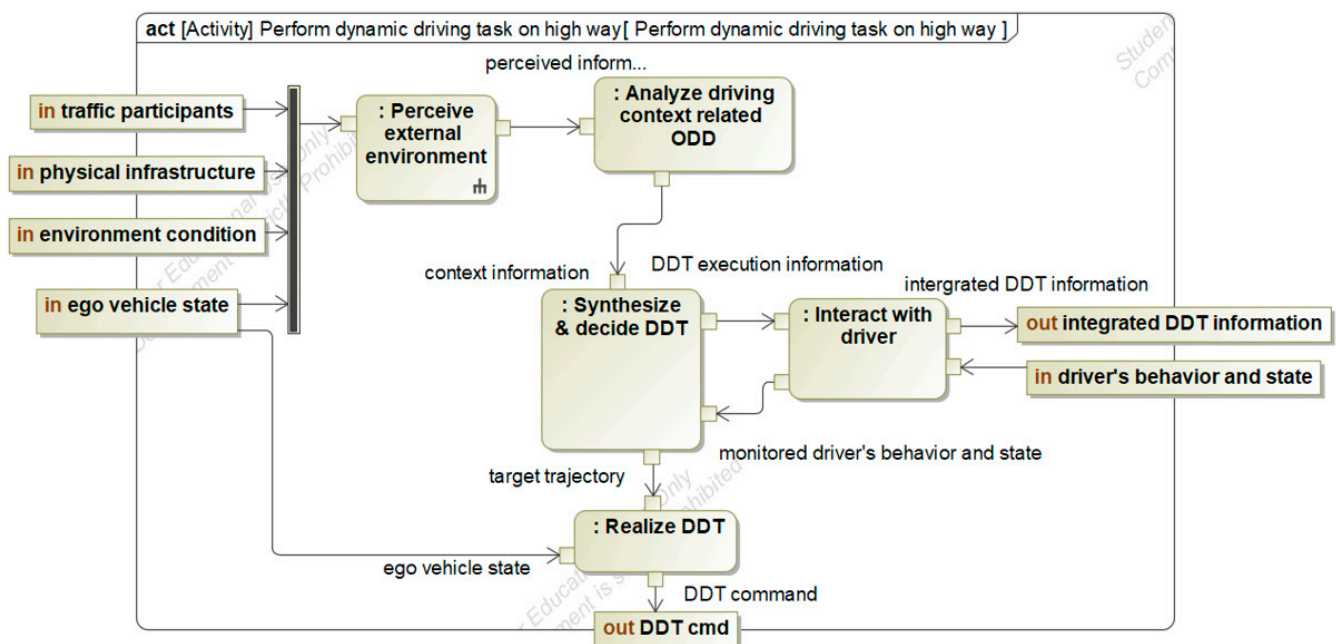


Figure 1. Behavior of ADS “Perform dynamic driving task on highway”.

This behavior model forms the basis for the subsequent HAZOP analysis, which focuses on sensor-failure scenarios.

As shown in Figure 1, the behavior model is structured into five primary actions:

- (1) *Perceive external environment*,
- (2) *Analyze driving context related to ODD*,

- (3) *Synthesize and decide DDT*,
- (4) *Realize DDT*,
- (5) *Interact with driver*.

The first action, *Perceive external environment*, is essential for acquiring both ego-state information (e.g., velocity, acceleration, steering angle) and external inputs, including environmental conditions (e.g., weather), traffic participants (surrounding vehicles and obstacles), and physical infrastructure (e.g., signals, lane markings, and road shoulders).

The second action, *Analyze driving context relative to the ODD*, interprets the perceived information to determine whether current driving conditions fall within the predefined ODD.

The *Synthesize & decide the DDT* action builds on the contextual understanding obtained from the previous step. Here, the ADS performs mission planning by integrating the current driving context with navigation objectives and operational constraints. This involves evaluating the positions, relative distances, and velocities of surrounding traffic participants to enable safe, context-aware planning. Multiple candidate driving tasks are generated, and the most suitable one is selected based on situational analysis.

Following task selection, the ADS conducts path planning and generates a target trajectory for the *Realize DDT* action. In this step, the *Realize DDT* action, the target trajectory with the current ego-vehicle state to produce executable control commands for acceleration, braking, and steering. These commands are transmitted to the vehicle actuators to physically realize the selected driving task, achieving closed-loop execution of the DDT.

The *Interact with Driver* action manages information exchange between the ADS and the human driver, presenting the current state of automated driving. This function is critical for initiating takeover requests, prompting the driver to resume control when the ADS determines that continued automated operation is unsafe. The execution of MRMs is also coordinated through these interactions.

The behaviors of individual sensors—light detection and ranging (LiDAR), Radar, and camera—are structured as internal function flows within the *Perceive external environment* action, as illustrated in Figure 2.

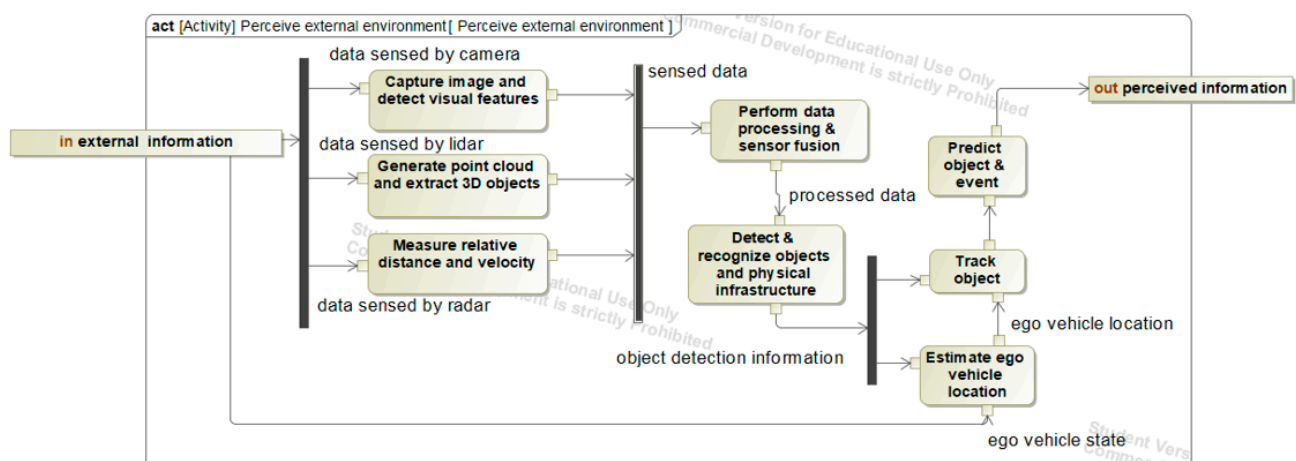


Figure 2. Activity diagram of *Perceive external environment* action.

Although Global Navigation Satellite System (GNSS) is commonly used in automated driving for perception and localization, it relies on external signals and is limited in environments with poor connectivity (e.g., tunnels, urban canyons). Consequently, GNSS-based

modules are excluded from this model to focus on LiDAR, radar, and cameras—the core onboard sensors of ADSs:

- Camera: It captures visual scenes and detects semantic features, including traffic signs, lane markings, and boundaries of traffic participants.
- LiDAR: It generates high-resolution three-dimensional (3D) point clouds and extracts geometrical information to construct spatial maps and detect 3D objects.
- Radar: It measures the relative distance and velocity of the surrounding traffic participants, providing robust motion data under low-visibility conditions such as fog or darkness.

The data from these three sensor modalities are processed in the *Perform data processing and sensor fusion* action, where multi-sensor information is temporally and spatially aligned. Sensor fusion leverages the complementary strengths of each sensor to enhance perception performance, enabling the ADS to detect and recognize surrounding traffic participants (e.g., vehicles and static obstacles) and physical infrastructure (e.g., signals, road markings, and road shoulders), as well as to estimate the ego vehicle's location.

Traffic participants are further tracked over time, allowing the ADS to anticipate potential events and, in certain scenarios, perform behavior analysis and prediction. Sensor failures can compromise the detection of critical information, thereby reducing the accuracy and reliability of subsequent activities that depend on these inputs.

2.2. Summary of Sensor Capabilities

To further examine the contributions of the three sensor types shown in Figure 2, a planar sensor placement model is constructed to illustrate how 360° perception is achieved by the ADS. In this study, the configuration depicted in Figure 3 is adopted, in which the ego vehicle is equipped with one LiDAR, eight Radars (one long-range, two mid-range, and five short-range), and four cameras. Table 1 summarizes the properties of each sensor, including horizontal field of view (HFOV), sensing range, and, for LiDAR and Radar, the accuracy of relative distance and velocity measurements [22–27].

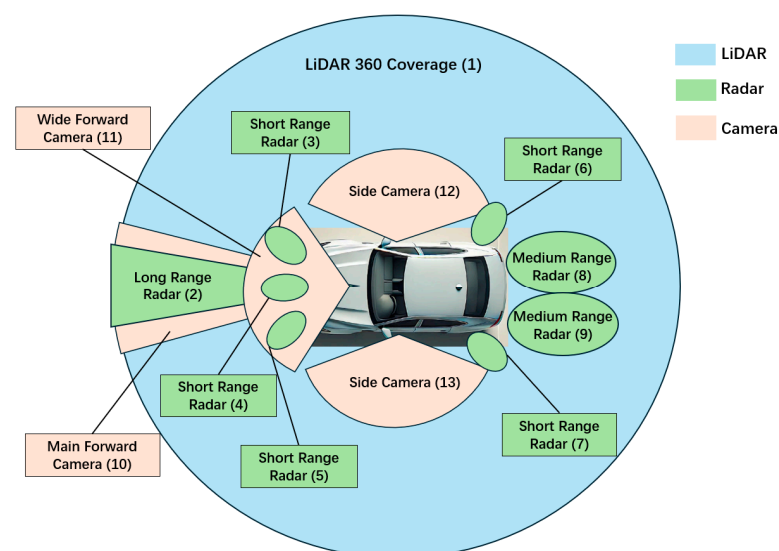


Figure 3. Sensor configuration.

Table 1. Overview of sensor capabilities.

	LiDAR (1)	Long- Range Radar (2)	Short- Range Radar (3)	Short- Range Radar (4)	Short- Range Radar (5)	Short- Range Radar (6)	Short- Range Radar (7)	Medium- Range Radar (8)	Medium- Range Radar (9)	Main For- ward Cam- era (10)	Wide For- ward Cam- era (11)	Side Cam- era (12)	Side Cam- era (13)
HFOV	360°	40°	50°	50°	50°	50°	50°	50°	50°	50°	150°	150°	150°
Sensing range (m)	0–200	0–200	0–20	0–20	0–20	0–20	0–20	0–80	0–80	0–200	0–50	0–50	0–50
Distance accuracy (m)	±0.05	±1–3	±0.24	±0.24	±0.24	±0.24	±0.24	±0.4	±0.4				
Velocity accuracy (km/h)	±3	±2.7	±1.0	±1.0	±1.0	±1.0	±1.0	±2.0	±2.0				
Lane markings	N	N	N	N	N	N	N	N	N	Y	Y	N	N
Road shoulder	Classification	Y	N	N	N	N	N	N	N	Y	Y	Y	N
	Relative distance and velocity	Y	Y	Y	N	N	Y	N	Y	N	N	N	N
In-lane front traffic participant	Classification	N	N	N	N	N	N	N	N	Y	Y	N	N
	Relative distance and velocity	Y	Y	Y	Y	Y	N	N	N	N	N	N	N
In-lane rear traffic participant	Classification	N	N	N	N	N	N	N	N	N	N	N	N
	Relative distance and velocity	Y	N	N	N	N	N	N	Y	Y	N	N	N
Right-lane traffic participant	Classification	N	N	N	N	N	N	N	N	Y	Y	Y	N
	Relative distance and velocity	Y	Y	Y	Y	N	Y	N	Y	N	N	N	N
Left-lane traffic participant	Classification	N	N	N	N	N	N	N	N	Y	Y	N	Y
	Relative distance and velocity	Y	Y	N	Y	Y	N	Y	N	Y	N	N	N

Note: Y indicates “available”, and N indicates “not available”.

Based on the behavior model and MRM requirements outlined in relevant standards [3,6], the minimal set of information required for MRM execution is extracted from the “perceived information” output of the *Perceive external environment* action. Table 1 indicates each sensor’s ability to provide the corresponding information as “Y” (available) or “N” (not available), based on its functional capabilities and mounting position shown in Figure 3.

While LiDAR is primarily used for high-resolution 3D mapping and distance estimation, its function in this study is extended to approximate relative velocity by tracking the displacement of traffic participants across consecutive time steps [22]. This assumption enhances sensor utility, particularly for obstacle detection and surface recognition.

The information required for MRM execution includes “traffic participants,” “road markings,” and “road shoulders.”

For “traffic participants,” dynamic and static vehicles or obstacles in the current lane (front and rear) and adjacent lanes (left and right) are considered, as they are most relevant to MRM decision-making. For each participant, the classification, relative distance, and relative velocity with respect to the ego vehicle are extracted.

Since traffic participants are categorized by their lane-relative positions (in-lane, left-lane, right-lane), a “Y” indicates that the corresponding sensor can potentially acquire this information. The specific sensor detecting a given traffic participant depends on its relative position to the ego vehicle and the sensor coverage illustrated in Figure 3.

“Road markings,” extracted from physical infrastructure, play a critical role in MRM scenarios involving lane keeping and lane changes. Lane markings are first detected during the *Perceive external environment* action and then utilized in the *Synthesize & decide DDT* action for trajectory planning. For lane keeping, they ensure alignment with the current lane center. For lane changes, lane markings are used in the *Analyze driving context related to ODD* action to identify the current and target lanes and subsequently generate a feasible lane-change trajectory in the *Synthesize & decide DDT* action.

Information about the road shoulder is also required when the ADS executes a lane change toward the road shoulder during MRM execution. The system must assess its suitability by recognizing shoulder boundaries and detecting potential barriers (e.g., guardrails, walls), along with their relative distance and velocity with respect to the ego vehicle.

2.3. HAZOP Analysis

Based on the behavior model and sensor capability analysis in Sections 2.1 and 2.2, a HAZOP analysis is conducted. Rather than analyzing sensor failures at the individual sensor level, the HAZOP analysis adopts an information-level perspective. Multiple sensors may contribute to the same perceptual function required for MRM execution, such as lane markings, road shoulder, or surrounding traffic participants. Therefore, combinations of sensor failures are analyzed based on their cumulative impact on the availability of these minimal information elements, rather than on isolated sensor faults.

In this analysis, sensor failure is defined as a complete loss of function, meaning that no data can be obtained from the sensor. The assumed environment is a highway scenario conforming to international design standards, with the road shoulder on the right.

The analysis evaluates how sensor failures impact the minimal set of information required for MRM execution—lane markings, road shoulder, and traffic participants—using the HAZOP guide words “No” and “Part of.” The “No” category represents scenarios in which all relevant sensors fail, making the information entirely unavailable. The “Part of” category addresses partial information loss due to the failure of one among multiple contributing sensors [8,28].

As shown in Table 2, the identified hazards are further analyzed to determine potential hazardous events. The term “risk” in this analysis is used in a qualitative sense to describe the exposure to potential events and consequences and is not intended to represent the associated likelihood of occurrence [28].

Each hazard is qualitatively categorized into three types (H1, H2, H3) based on its potential risk to MRM behavior:

- Hazard Type 1 (H1): The risk associated with lateral control during lane changes. Depending on the type of sensor failure, the lane change may involve only the left lane, only the right lane, or both.
- Hazard Type 2 (H2): The risk associated with lateral control during both lane changes and lane keeping.
- Hazard Type 3 (H3): The risk associated with longitudinal control.

H1 and H2 pertain to lateral control, while H3 concerns longitudinal control. In cases of multiple simultaneous sensor failures, combined risks may occur, such as H1 with H3 or H2 with H3.

In “Part of” cases, the impact of individual sensor failures (LiDAR and Radar) on traffic participant detection is analyzed separately. Failures limited to cameras, which may only impair traffic participant classification, are not considered hazardous events for MRM execution and are therefore excluded from the analysis. For combined failures of LiDAR and Radar affecting a traffic participant, the corresponding hazardous event and Hazard Type defined under the “No” category can be directly applied.

Table 2. Results of HAZOP Analysis on the Impact of Sensor Failures on MRM Execution.

Guide Words	Hazard	Potential Hazardous Events	Hazard Type
No	Loss of lane marking detection	Unintended lateral deviation due to lane marking detection failure, potentially causing lane departure or road exit as well as posing a high safety risk to the ego vehicle and surrounding traffic.	H2
	Loss of road-shoulder detection	Causing misestimation of drivable boundaries and stopping zones, potentially leading to unsafe stops or collisions with roadside barriers as well as posing a high safety risk to the ego vehicle and surrounding traffic during right-lane change to the shoulder.	H1
	Loss of in-lane front traffic participants detection	When a static obstacle is ahead or a vehicle brakes suddenly, failure of the ADS to perceive the event and decelerate properly may result in a rear-end collision.	H3
	Loss of in-lane rear traffic participant detection	When a following vehicle fails to decelerate in response to ego braking, failure of the ADS to detect this behavior and adjust longitudinal control may result in a collision.	H3
	Loss of right-lane traffic participant detection	When a vehicle or obstacle is present in the right lane, ADS failure to detect it may lead to an incorrect right-lane change decision and result in a collision.	H1
	Loss of left-lane traffic participant detection	When a vehicle or obstacle is present in the left lane, ADS failure to detect it may lead to an incorrect left-lane change decision and result in a collision.	H1
Part of	Traffic participants: Incomplete measurement of relative distance and velocity (LiDAR failure)	When a vehicle is present in the ego or adjacent lane, ADS errors in estimating its relative velocity may lead to incorrect longitudinal and lateral control, resulting in a potential collision.	H1/H3
	Incomplete measurement of relative distance and velocity (Radar failure)	When a vehicle is present in the ego or adjacent lane, ADS errors in estimating its relative distance and orientation may lead to incorrect longitudinal and lateral control, resulting in a potential collision.	H1/H3

By referencing Figure 3, Tables 1 and 2, the hazards associated with any combination of sensor failures can be identified. The final risk to MRM behavior is then evaluated based on the cumulative impact of the corresponding hazard types.

2.4. Discussion of the HAZOP Analysis Results

The HAZOP analysis in this section systematically identifies hazards arising from various sensor-failure combinations in highway-driving ADS. As characterized in IEC 61882, HAZOP is inherently a qualitative, guide-word-based method for systematic hazard identification and is therefore applied in this work at a structural level to identify hazardous situations. It is not intended to model dynamic or non-linear system behaviors [28].

For multiple sensor failures, Tables 1 and 2 are used to determine which information becomes unavailable and how these losses correspond to potential risks during MRM execution. Hazards are classified into three types (H1, H2, H3), representing risks associated with lateral and longitudinal control.

Based on the analysis, the following considerations are derived for camera failures:

- Front-side camera failure: Prevents detection of lane markings, compromising lateral control. Consequently, both lane-keeping and lane-change maneuvers are not recommended during MRM execution.
- Right-side camera failure: Impairs assessment of road-shoulder usability. Therefore, rightward lane changes targeting the shoulder should be avoided.

For traffic participant detection, which primarily relies on both LiDAR and Radar, sensor failures can significantly compromise MRM execution:

- Failure of either LiDAR or Radar: Detection must rely solely on the remaining sensor, often resulting in substantial errors in estimating relative distance and velocity (as summarized in Table 1), potentially leading to unsafe control decisions.
- Simultaneous failure of both LiDAR and Radar: This creates a blind area in which traffic participants cannot be perceived. If a participant is present, the ADS lacks critical distance and velocity information, increasing the risk of hazardous decisions during MRM execution.

Considering these hazardous events and the three hazard types categorized in Table 2, the following section proposes a strategy to mitigate such incidents and reduce risks associated with MRM execution under sensor-failure conditions.

3. MRM Strategy

3.1. Activity Diagram

To address the challenges identified in Section 2, this section presents an MRM strategy designed to mitigate potential hazards arising from sensor failures. The activity of the proposed MRM strategy is illustrated in Figure 4.

The MRM strategy is implemented as part of the *Synthesize & decide DDT* action in the ADS behavior model, as described in Section 2. It functions as a response mechanism activated when the ADS determines that an MRM must be executed under sensor-failure conditions. Compared to the original activity, this strategy incorporates an additional input, “sensor condition,” which conveys the status of each sensor, including the capabilities listed in Table 1 and the current availability or failure of each sensor.

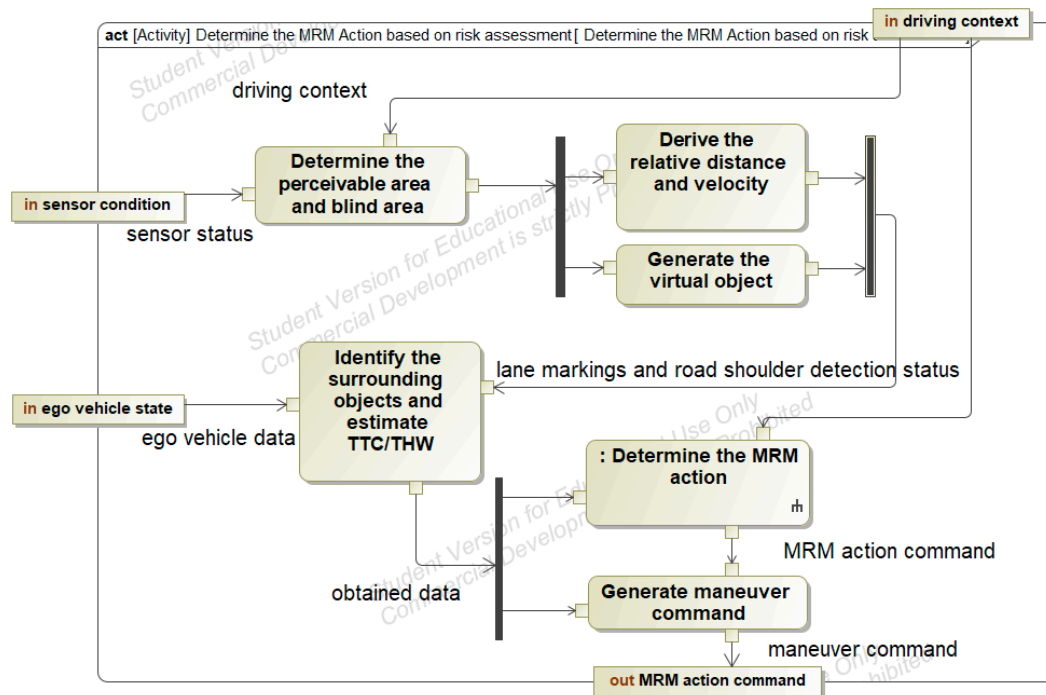


Figure 4. MRM strategy: activity diagram of the *Determine MRM action based on risk assessment*.

3.2. Actions in the MRM Strategy

The proposed MRM strategy consists of six main actions:

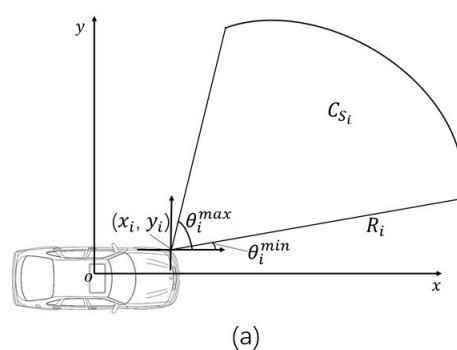
1. *Determine the perceivable and blind area,*
2. *Derive the relative distance and velocity,*
3. *Generate the virtual object,*
4. *Identify the surrounding objects and estimate TTC/THW,*
5. *Determine the MRM action, and*
6. *Generate maneuver command.*

Each action is described in detail in the following subsections.

3.2.1. Determine the Perceivable Area and Blind Area

Based on the sensor condition, the perceivable area and blind zones are determined in the two-dimensional (2D) Cartesian vehicle coordinate system shown in Figure 5. Each sensor S_i has a predefined mounting position (x_i, y_i) , as illustrated in Figure 3 ($i \in [1, 9]$, corresponding to the sensor numbering in the figure).

Example: Radar S_i is active ($i \in [2, 9]$)



Example: LiDAR S_1 and Radar S_i fail ($i \in [2, 9]$)

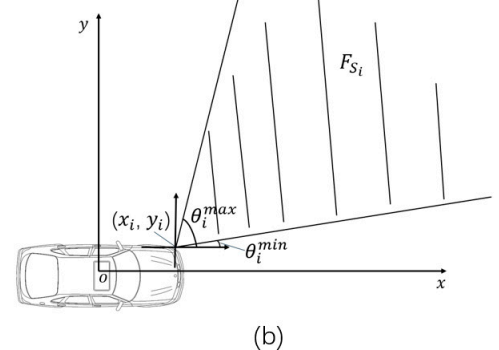


Figure 5. Examples of a 2D Cartesian vehicle coordinate system for (a) perceivable areas when S_i is active and (b) blind areas when both LiDAR S_1 and Radar S_i ($i \in [2, 9]$) fail.

A polar coordinate frame is defined at each sensor's mounting location. For each sensor S_i , the HFOV and range (R_i) are defined according to Table 1, and the angular coverage $[\theta_i^{min}, \theta_i^{max}]$ is determined based on its HFOV and orientation relative to the ego vehicle's heading.

If sensor S_i is active ($S_i \in S_{active}$), its perceivable area in the coordinate system is defined as follows:

$$C_{S_i} = \left\{ (x, y) \left| \begin{array}{l} \sqrt{(x - x_i)^2 + (y - y_i)^2} \leq R_i, \\ \theta_i^{min} \leq \tan^{-1} \left(\frac{y - y_i}{x - x_i} \right) \leq \theta_i^{max} \end{array} \right. \right\}, S_i \in S_{active} \quad (1)$$

When the LiDAR sensor S_1 and any one or more of the Radar sensors S_i ($i \in [2, 9]$) fail simultaneously, the resulting blind area can be defined as follows:

$$F_{S_i} = \left\{ (x, y) \left| \theta_i^{min} \leq \tan^{-1} \left(\frac{y - y_i}{x - x_i} \right) \leq \theta_i^{max} \right. \right\}, S_i \in S_{fail} \quad (2)$$

where S_{fail} denotes the set of failed Radar sensors.

3.2.2. Derive the Relative Distance and Velocity

The sensing data from the remaining functional sensors is evaluated by comparing each traffic participant's position with the perceivable area C_{S_i} . This determines whether a traffic participant is detected by both sensor types—LiDAR and Radar—or by only one type.

If a participant is detected by only one sensor type, it is considered to have potential perception errors. The relative distance and velocity of such an object are computed as

$$\tilde{d}_n(t) = d_n(t) - \varepsilon_{i,r}, \tilde{v}_n(t) = v_n(t) - \varepsilon_{i,v}, \quad (3)$$

where $\varepsilon_{i,r}$ and $\varepsilon_{i,v}$ are the positive distance and velocity errors associated with sensor S_i , as specified in Table 1. To account for worst-case risk, the relative distance and velocity are reduced by applying the corresponding sensor errors.

3.2.3. Generate Virtual Object

When a blind area F_{S_i} is present, a virtual object is generated within the corresponding lane segment covered by the blind area, as illustrated in Figure 6.

The virtual object generated in each relevant lane is defined as follows:

- Right/left lanes: The virtual object is assumed to move in the same direction and at the same speed as the ego vehicle, resulting in zero relative velocity.
- In-lane front: The virtual object is positioned at the last recorded location of the front vehicle or obstacle prior to sensor failure, with velocity set to zero. If no front vehicle was previously detected, the object is placed 200 m ahead of the ego vehicle.
- In-lane rear: The virtual object is positioned at the last recorded location of the rear vehicle prior to sensor failure, with velocity set to the lane's maximum speed limit. If no rear vehicle was detected, it is placed 80 m behind the ego vehicle.

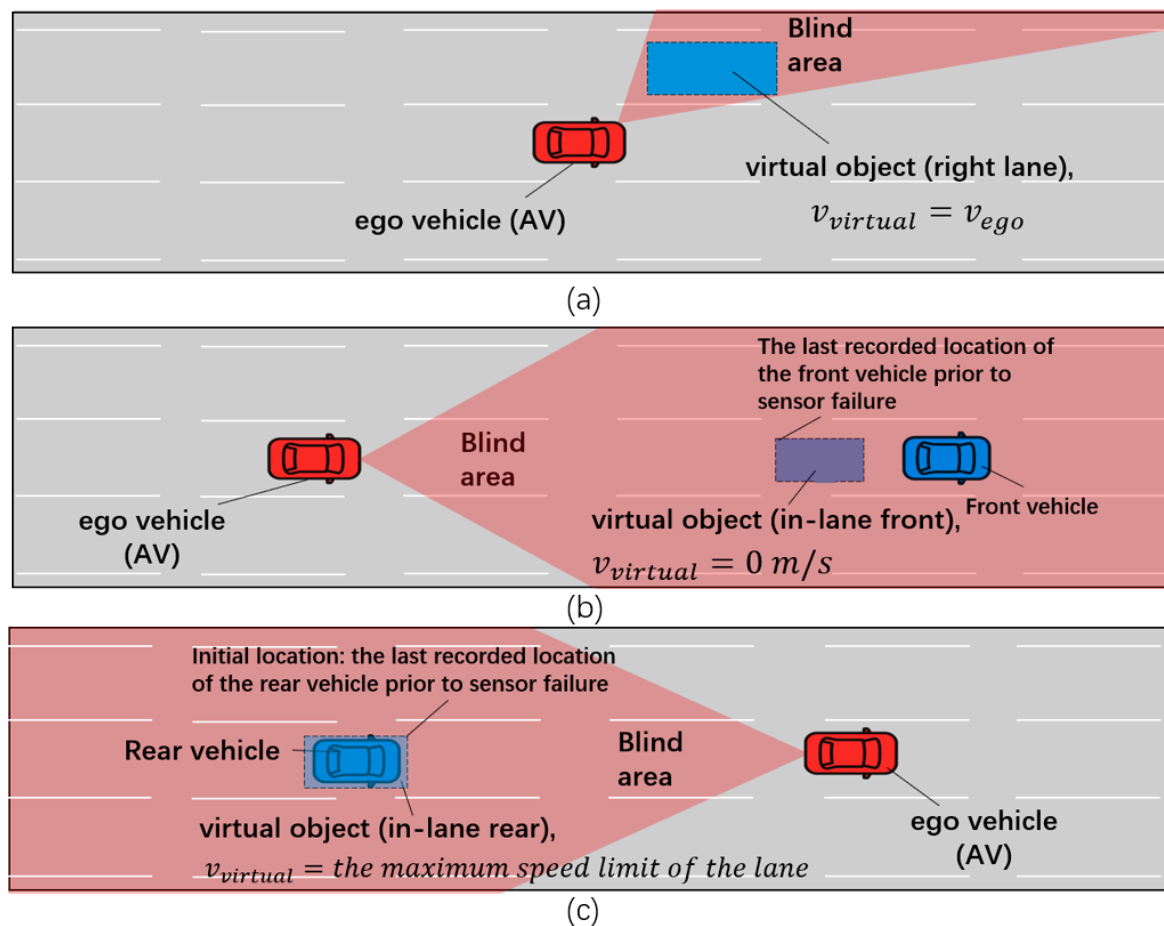


Figure 6. Generation of virtual objects (a) in the right lane, (b) in front of the current lane, and (c) behind the current lane.

The parameters of the virtual objects are determined based on conservative worst-case assumptions corresponding to each sensor-failure scenario. As illustrated in Figure 6, the virtual objects are not intended to represent specific real traffic participants but to characterize potentially hazardous regions within perception blind areas.

In case (a), the virtual object is defined only by its longitudinal extent within the affected lane and its velocity, representing the maximum possible vehicle length that could be present in the blind area from the perspective of the ego vehicle. For the front-lane scenario in case (b), the position and velocity of the virtual object are considered to reflect situations in which a preceding vehicle may suddenly decelerate, or an unexpected obstacle may appear immediately after sensor failure. When no front object is detected prior to failure, a stationary virtual object is placed 200 m ahead of the ego vehicle, corresponding to the maximum reliable detection range of the front sensor and representing a conservative assumption that a hazardous obstacle may exist just beyond the perception limit. For the rear-lane scenario in case (c), the virtual object is configured to represent a following vehicle whose driver reacts slowly and does not provide sufficient deceleration margin for the ego vehicle.

In the current implementation, the virtual object model focuses on longitudinal distance, relative velocity, and lane association (ego, left, or right lane). Lateral dimensions and object width are not explicitly considered, as the objective at this stage is to capture conservative longitudinal and lane-change-related collision risk under sensor failure, rather than detailed object geometry.

3.2.4. Identify the Surrounding Objects and Estimate TTC/THW

This action identifies the surrounding objects critical for the ego vehicle's current MRM decision-making, including both sensed traffic participants and generated virtual objects. In this study, six closest surrounding objects are considered relevant: the in-lane front object, in-lane rear object, right-lane front object, right-lane rear object, left-lane front object, and left-lane rear object.

Each object may be either a real object with derived relative distance and velocity or a virtual object generated due to sensor failure. The TTC and THW of these relevant objects are estimated for risk assessment in the MRM decision-making process:

$$TTC(t) = \begin{cases} \frac{D(t)}{|V(t)|}, & V(t) < 0 \\ \infty, & V(t) \geq 0 \end{cases} \quad (4)$$

$$THW(t) = \frac{D(t)}{v_{ego}(t)}, \quad (5)$$

where $D(t)$ is the relative distance between the ego vehicle and the object, $V(t)$ is the relative velocity of the object with respect to the ego vehicle (negative if approaching), and $v_{ego}(t)$ is the ego vehicle's speed.

THW is applied only to front objects to maintain a safe following distance for the ego vehicle, particularly in situations where a relatively small velocity could result in an excessively large TTC, making risk estimation less reliable.

3.2.5. Determine the MRM Action and Generate Maneuver Command

The appropriate MRM action is determined through the decision-making process illustrated in Figure 7, which accounts for the current sensor-failure status and surrounding driving environment. This process evaluates the availability of lane marking and road-shoulder information, as well as data from surrounding object identification and TTC/THW estimation, including object types and their corresponding TTC/THW values (used, for example, in the *Check right-lane change feasibility* action step). Based on the selected MRM action and the estimated TTC/THW values, specific deceleration and steering commands are generated in the *Generate maneuver command* action.

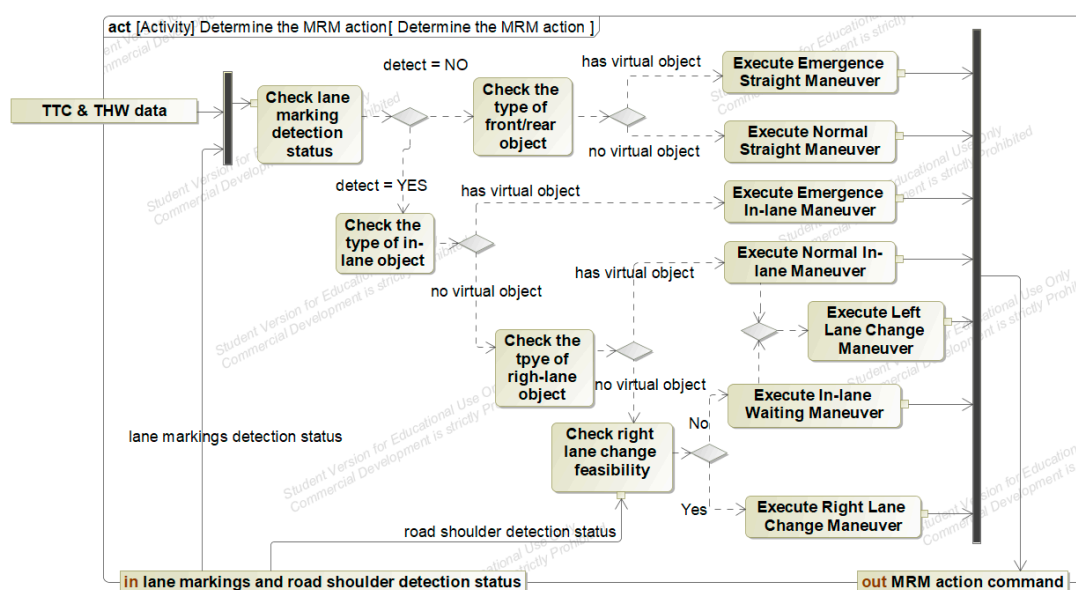


Figure 7. Determination of MRM action in the MRM strategy.

As shown in Figure 7, the determined MRM action is classified into one of seven action types. These types are defined with reference to the identified hazards and potential hazardous events, corresponding to the three hazard types (H1, H2, H3) described in Section 2. The seven MRM action types are defined as follows:

1. *Normal Straight Maneuver*: A longitudinal-only maneuver involving deceleration or speed maintenance based on front and rear detected objects. This maneuver corresponds to sensor-failure conditions associated with H2.
2. *Emergency Straight Maneuver*: A longitudinal-only maneuver involving deceleration or speed maintenance, accounting for both detected and virtual objects generated under simultaneous LiDAR and Radar failures. This maneuver corresponds to sensor-failure conditions associated with the combination of H2 and H3.
3. *Normal In-lane Maneuver*: A longitudinal and lateral maneuver restricted to deceleration, speed maintenance, and lane keeping based on in-lane detected objects. This maneuver corresponds to sensor-failure conditions associated with H1, specifically where lateral control for a right-lane change is at risk.
4. *Emergency In-lane Maneuver*: A longitudinal and lateral maneuver involving deceleration, speed maintenance, and lane keeping, accounting for both in-lane detected objects and virtual objects generated under simultaneous LiDAR and Radar failures. This maneuver corresponds to sensor-failure conditions associated with the combination of H1 and H3.
5. *In-lane Waiting Maneuver*: A longitudinal and lateral maneuver involving deceleration, speed maintenance, and lane keeping based on in-lane detected objects, while waiting for an opportunity to perform a right-lane change. This maneuver applies when no hazards (H1, H2, H3) occur, or when H1 is limited to left-lane changes. If lane-change conditions are not met, the vehicle decelerates to a predefined threshold speed and maintains it while waiting. The speed-holding phase is limited to an additional travel distance of 200 m—the maximum reliably perceived range prior to sensor failure—to ensure safety.
6. *Right-lane Change Maneuver*: A longitudinal and lateral maneuver involving deceleration, speed maintenance, and a right-lane change. This maneuver applies when no hazards (H1, H2, H3) are present, or when H1 is limited to left-lane changes.
7. *Left-lane Change Maneuver*: A longitudinal and lateral maneuver involving deceleration, speed maintenance, and a left-lane change. This maneuver applies when no hazards (H1, H2, H3) are present, or when H1 is limited to right-lane changes.

TTC thresholds for front and rear objects are set to 5 s, and the THW threshold for front objects is set to 2 s. Ego vehicle deceleration is discretized into four levels: 0, -2 , -4 , and -6 m/s² [29–31]. In the proposed MRM strategy, when both front and rear objects (real or virtual) are present, priority is given to minimizing collision risk with the front object in accordance with traffic liability regulations, while mitigating rear collision risk as much as possible within this constraint.

For the *Normal In-lane Maneuver* and *In-lane Waiting Maneuver*,

- If both front and rear objects satisfy their TTC/THW thresholds, a deceleration of -2 m/s² is applied.
- If the front object violates any threshold, a deceleration of -4 m/s² is applied.
- If only the rear object violates its threshold, the ego vehicle maintains its current speed (0 m/s²).

For *Right-lane Change Maneuver* and *Left-lane Change Maneuver*, execution requires

- TTC and THW with the target lane's front object exceed the respective thresholds, and
- No rear object is detected in the target lane.

For the *Right-lane Change Maneuver*, the proposed strategy prioritizes executing the lane change when it is determined feasible. In the case where the target lane for a right-lane change is the road shoulder, the maneuver is permitted only if the shoulder is detected and classified as a safe stopping area. Unlike the *Right-lane Change Maneuver*, the *Left-lane Change Maneuver* is a special case considered when there is a rear-end collision risk in the current lane and a safe escape to the left is available.

The remaining two MRM types—*Emergency Straight Maneuver* and *Emergency In-lane Maneuver*—must account for both detected and virtual objects.

1. Case: Virtual object in front

To avoid entering a blind area with a virtual in-lane front object, the deceleration $a_{calc}(t)$ is calculated as follows:

$$a_{calc}(t) = \frac{-v_{ego}^2(t)}{2(D_{front} - \Delta x_{ego}(t))(1 - S_m)}, \quad (6)$$

$$a_{req}(t) = \begin{cases} -2, & \text{if } a_{calc}(t) \geq -2 \\ a_{calc}(t), & \text{if } -6 < a_{calc}(t) < -2 \\ -6, & \text{if } a_{calc}(t) \leq -6 \end{cases}, \quad (7)$$

where $v_{ego}(t)$ denotes the ego vehicle's velocity, D_{front} denotes the last recorded relative distance to the front vehicle before sensor failure, and $\Delta x_{ego}(t)$ denotes the ego vehicle's longitudinal displacement since the start of MRM execution. A 10% safety margin S_m is applied to account for uncertainties. The final required deceleration $a_{req}(t)$ is constrained to the range $[-6, -2]$ m/s² to ensure vehicle stability.

- If no rear object is detected, $a_{req}(t)$ is applied.
- When a rear object is detected and TTC is less than 5 s,
 - (a) When $a_{req}(t) > -4$, the current speed is maintained to provide the following vehicle with additional reaction time.
 - (b) When $a_{req}(t) \leq -4$, the deceleration $a_{req}(t)$ is applied, prioritizing the forward collision risk.

2. Case: Virtual object in rear

If the in-lane rear object is virtual,

- If no front object is detected or either TTC or THW exceeds its threshold, the current speed is maintained during the first 5 s of MRM execution to allow sufficient reaction time for potential following vehicles. During this period, the MRM execution status is broadcast via the eHMI.
- When a real front object is detected and either TTC or THW falls below the threshold during the initial phase, deceleration is initiated. The deceleration continues until TTC and THW exceed their thresholds, at which point the speed-maintaining strategy resumes.

3. Case: Virtual object in front and rear

If both the in-lane front and rear objects are virtual,

- When $a_{req}(t) > -4$, the current speed is maintained during the first 5 s of MRM execution.
- Otherwise, the deceleration $a_{req}(t)$ is applied to mitigate the front collision risk

The proposed MRM strategy considers not only the current driving environment but also the specific consequences of partial sensor failures, as identified through the HAZOP analysis. By integrating these two aspects, the strategy enables the ADS to make optimal decisions during MRM execution at each time step.

3.3. Implementation of the MRM Strategy

In this study, the proposed MRM strategy is implemented in MATLAB (version R2024b), as illustrated in Figure 8. The simulation framework computes perceivable and blind areas based on specified sensor-failure conditions, as well as the sensor configurations and capabilities summarized in Figure 3 and Table 1. It incorporates object data derivation, virtual object generation, and algorithmic execution of the MRM decision-making process.

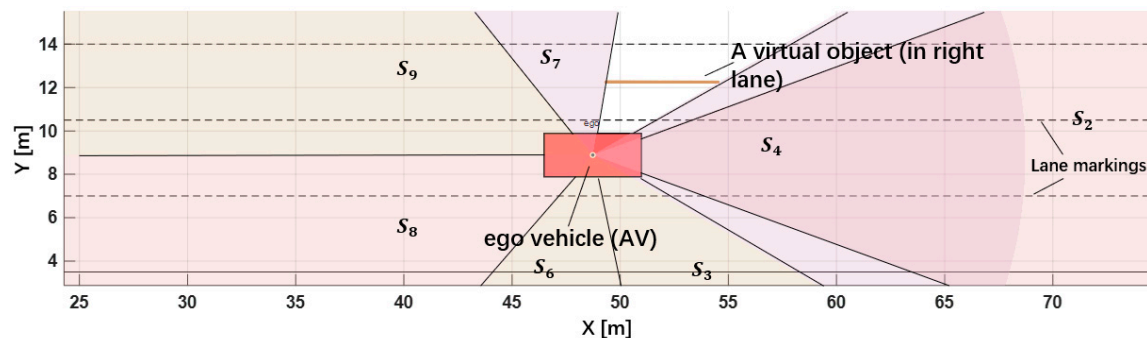


Figure 8. A simulation example under LiDAR S_1 and Radar S_3 is applied to mitigate the front collision risk area, blind area, and a virtual object introduction.

To focus on decision-making, sensor perception modeling is simplified. All sensors are assumed to be located at the center of the ego vehicle, allowing unified geometric calculations without compromising the validity of the risk evaluation.

To verify the proposed MRM strategy, two scenarios derived from hazardous events and one scenario involving a safe road-shoulder stop are formulated and examined in the following section.

4. Simulation-Based Verification

4.1. Simulation Environment

This study employs a co-simulation environment integrating MATLAB (version R2024b) and CARLA (version 0.9.15) to verify and validate the proposed MRM strategy across three representative scenarios. CARLA, an open-source simulator widely used in automated driving research, was used to construct highway-driving scenarios, modeling both the ego vehicle and surrounding traffic participants with realistic dynamics. The simulation was based on the “Town04” map, providing a highway network, and the ego vehicle was instantiated using the CARLA blueprint “vehicle.audi.tt”. MATLAB was used to implement the decision-making algorithms, risk assessment modules, and the proposed MRM strategy.

A Python-based communication bridge (Python 3.9) was implemented using CARLA’s Python API to enable co-simulation with MATLAB [32–34]. Vehicle states in CARLA—including position, velocity, and orientation—were streamed to MATLAB at each simulation step with a 0.05 s sampling time. Sensor-failure conditions were preset for each scenario. MATLAB processed the received state information through the MRM decision-making framework to determine the appropriate maneuver. The resulting control commands—acceleration, braking, and steering—were transmitted back to CARLA via the same bridge.

Control commands were expressed in normalized values consistent with the CARLA vehicle control API: “throttle” and “brake” within [0.0, 1.0], and “steer” within [−1.0, 1.0]. A closed-loop control scheme was implemented in MATLAB to ensure stable maneuver execution. Specifically, a proportional-derivative (PD) controller regulated longitudinal control outputs: the acceleration command from the MRM decision logic was compared

with the actual acceleration feedback from CARLA, and the resulting error was iteratively corrected by adjusting the normalized throttle and brake values. This approach ensured that the ego vehicle's behavior in CARLA accurately reflected the intended MRM while accounting for simulator dynamics and response delays. Figure 9 illustrates an example visualization of the simulation scenario in the CARLA environment during MRM execution.



Figure 9. Example visualization of the simulation scenario in the CARLA environment during MRM execution. The red vehicle represents the ego vehicle, while the blue vehicles represent surrounding traffic participants.

Due to CARLA simulator constraints, the ego vehicle was considered stopped when its reported velocity reached 2 m/s; velocity outputs below this threshold are omitted from simulation results. This co-simulation setup, combining high-level decision-making in MATLAB with high-fidelity vehicle dynamics in CARLA, enabled a comprehensive and realistic evaluation of the proposed MRM strategy under diverse sensor-failure conditions.

4.2. Scenarios

To verify the proposed MRM strategy, three scenarios are selected, as illustrated in Figure 10. Scenarios A and B represent the most complex and characteristic cases identified from the hazardous event analysis, corresponding to sensor-failure conditions associated with the combination of H1 and H2. In both scenarios, simultaneous LiDAR and Radar failures create blind areas either in front of or behind the ego vehicle, while the vehicle must still navigate safely among surrounding traffic, making these cases critical for verification. Scenario C is designed to evaluate the strategy's ability to enable a safe road-shoulder stop when a rear vehicle is present in the right lane, under a failure condition associated with H1 but limited to left-lane changes.

4.2.1. Scenario A: Performing an MRM with a Virtual Object in Front and a Real Object Behind

Scenario A is defined based on the hazardous event described at the end of Section 2, in which a failure of front object detection triggers the initiation of an MRM execution. This is simulated by setting the LiDAR sensor and the two front-facing Radar sensors to a failure state. The initial scene assumes the ego vehicle traveling at 25 m/s, with a front vehicle 100 m ahead in the same lane and a rear vehicle approaching at 27 m/s from 50 m

behind. It is further assumed that the rear-vehicle driver reacts 2 s after the ego vehicle begins deceleration and communicates MRM execution information via the eHMI.

Simulation results are shown in Figure 11.

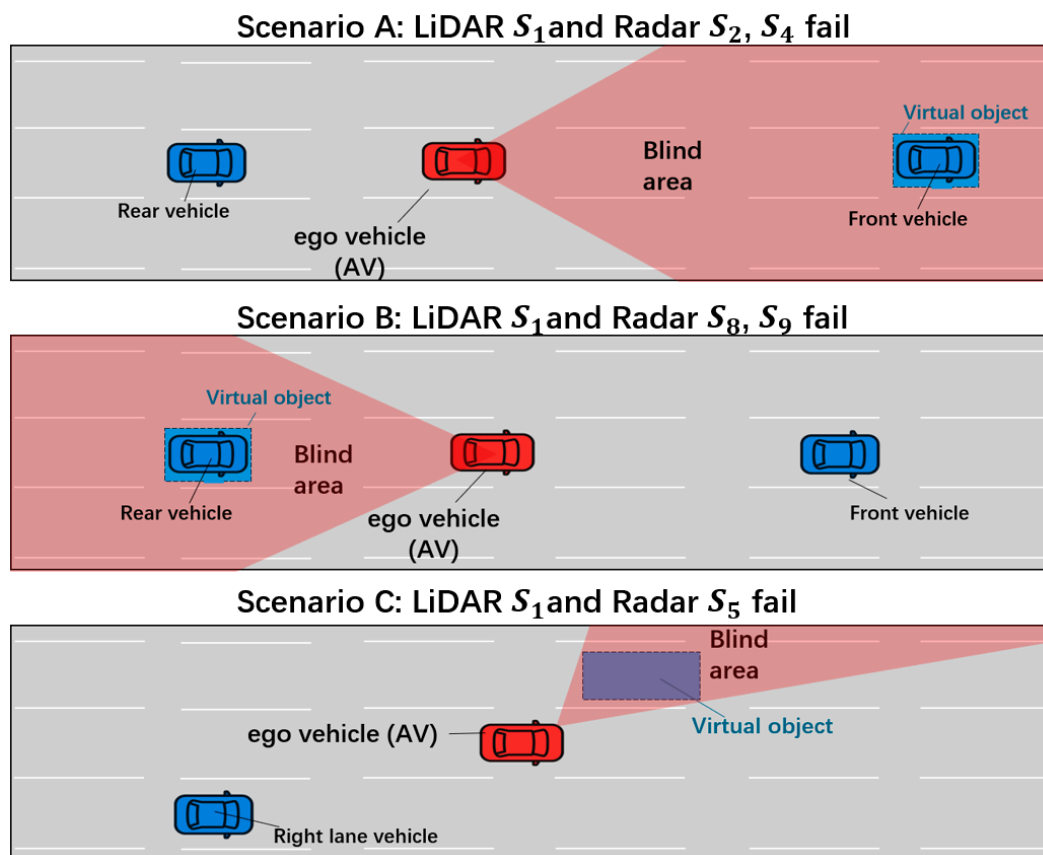


Figure 10. Scenario A, B and C.

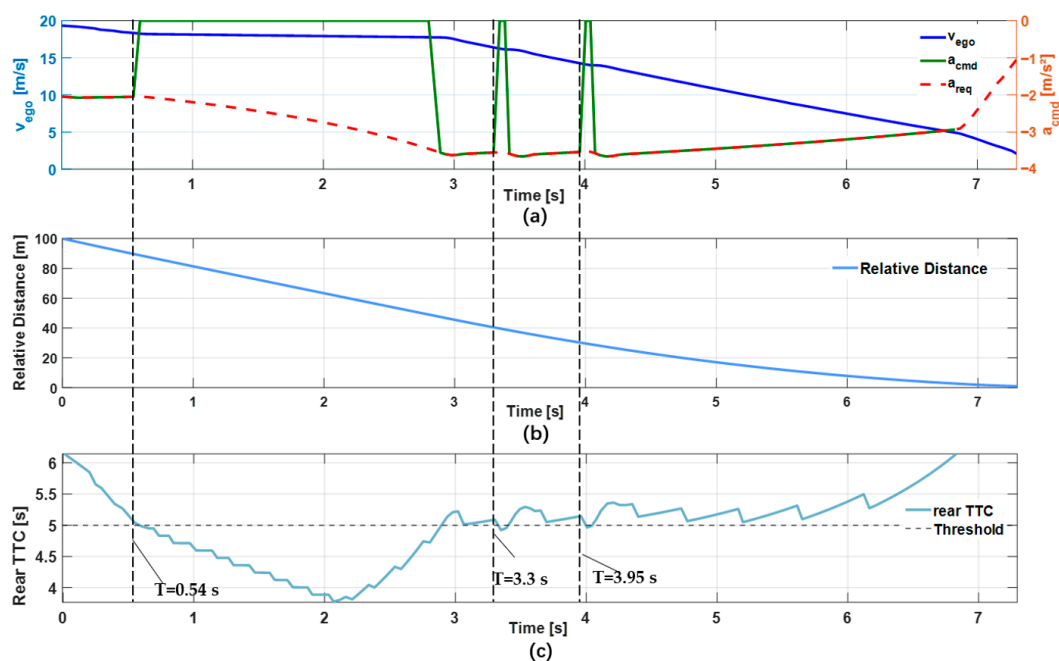


Figure 11. Result of simulation with Scenario A: (a) longitudinal velocity, required acceleration, and acceleration command of the ego vehicle; (b) relative distance to the front virtual object; (c) TTC with its threshold between the ego vehicle and the rear object.

According to the proposed MRM strategy, under this sensor-failure condition, the ADS executes an *Emergency in-lane maneuver*, prioritizing the front virtual object while also accounting for the detected rear object.

At $T = 0.54$ s, the first speed-maintenance phase was triggered as the rear TTC dropped below the threshold. The ego vehicle maintained its velocity until the TTC exceeded the threshold, after which it resumed deceleration according to the required acceleration profile a_{req} . Two additional speed-maintenance phases occurred at $T = 3.3$ s and $T = 3.95$ s in response to subsequent drops in rear TTC below the threshold. After the final recovery of TTC above the threshold, the ego vehicle continued decelerating according to a_{req} until coming to a complete stop. In this scenario, although the ego vehicle stopped in accordance with the MRM strategy, the short following distance of the rear vehicle resulted in a stopping position only 1.3 m ahead of the front virtual object.

4.2.2. Scenario B: Performing an MRM with a Virtual Object in the Rear and a Real Object in Front

Scenario B is defined based on the hazardous event concerning rear-object detection failure described at the end of Section 2, simulated by setting the LiDAR and two rear-facing Radar sensors to a failure state. The initial conditions assume the ego vehicle traveling at 22 m/s, with a fast-approaching rear vehicle 50 m behind at 30 m/s, and a leading vehicle 80 m ahead at 20 m/s. The rear-vehicle driver is assumed to react 2 s after the MRM notification via the ego vehicle's eHMI, decelerating at -4 m/s². The front vehicle is assumed to decelerate at -2 m/s² for the first 3 s, then accelerate to maintain a speed of 20 m/s.

Simulation results are shown in Figure 12. According to the proposed MRM strategy under this sensor-failure condition, the ADS executes an *Emergency in-lane maneuver*, prioritizing the detected front object while accounting for the rear virtual object.

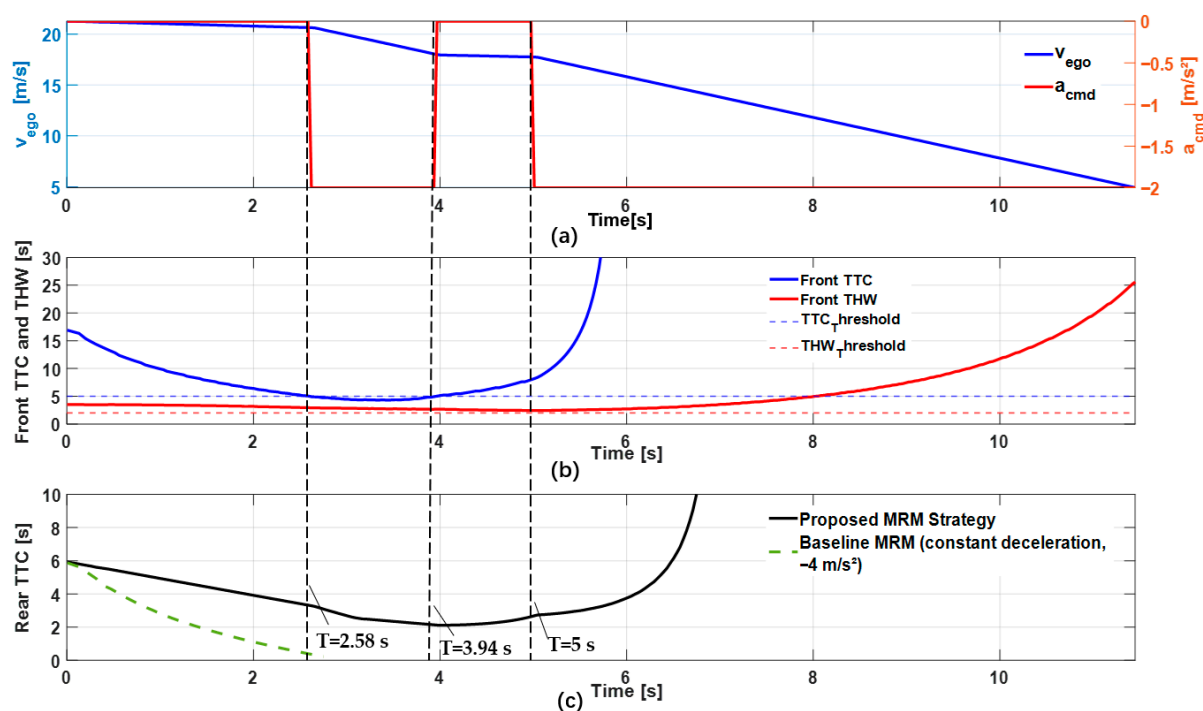


Figure 12. Result of simulation with Scenario B: (a) longitudinal velocity and acceleration command of the ego vehicle; (b) TTC and THW with their threshold between the ego and front vehicle; (c) TTC between the ego and rear vehicle, including a comparison with a baseline MRM strategy using a constant deceleration of -4 m/s².

The ego maintains its current speed while the TTC with the front vehicle satisfies the safety threshold, taking into account the presence of a rear vehicle and the potential hazard event associated with it. At $T = 2.58$ s, the ego vehicle begins decelerating in response to the front vehicle's slowing motion as the calculated TTC drops below the threshold. Speed maintenance is resumed at $T = 3.94$ s once the TTC recovers above the threshold. At $T = 5$ s, a continuous deceleration phase is initiated based on both TTC and THW indicators, and the ego vehicle continues to decelerate until coming to a complete stop. To further evaluate the effectiveness of the proposed strategy, a baseline MRM strategy is introduced for comparison in Scenario B. In the baseline approach, the ego vehicle initiates MRM execution and continuously decelerates at a constant rate of -4 m/s^2 , without adaptive consideration of potential hazard event associated with the rear vehicle. As shown in Figure 12c, the baseline strategy results in a rapid decrease in rear TTC, leading to a rear-end collision at $T = 2.75$ s. In contrast, the proposed MRM strategy dynamically alternates between speed maintenance and deceleration based on TTC and THW evaluation of front vehicle and the virtual object. This adaptive behavior allows the ego vehicle to avoid front collision while providing additional reaction time for the following vehicle, thereby mitigating a rear collision risk under the same scenario.

4.2.3. Scenario C: Performing an MRM Stop on Road Shoulder with a Virtual Object in the Left Lane

Scenario C illustrates the ego vehicle successfully performing Right-lane Changes toward the road shoulder and coming to a safe stop following the proposed MRM strategy. The sensor-failure condition is simulated by disabling the LiDAR and left-side Radar sensors; this configuration does not hinder the vehicle's ability to execute a *Right-lane change maneuver*. The initial setup assumes the ego vehicle traveling at 25 m/s in the middle lane of a three-lane highway adjacent to the road shoulder. A leading vehicle is positioned 50 m ahead in the same lane, traveling at 20 m/s , while a rear vehicle approaches in the adjacent right lane at a longitudinal distance of 50 m and a speed of 27 m/s .

The simulation results for Scenario C are shown in Figure 13.

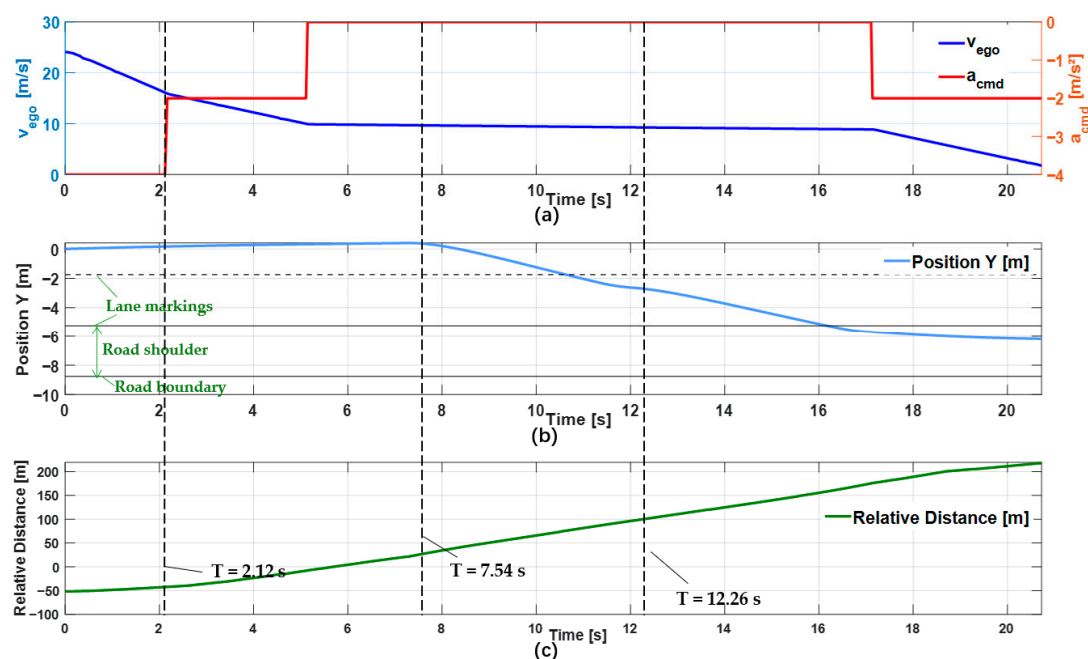


Figure 13. Result of simulation with Scenario C: (a) longitudinal velocity and acceleration command of the ego vehicle; (b) time-series of the ego vehicle's lateral position; (c) relative distance between the ego vehicle and right-lane rear object.

According to the proposed MRM strategy, the virtual object generated in the left-side blind area does not pose a risk to the right-lane change behavior; therefore, the ego vehicle performs the *In-lane waiting maneuver* in accordance with the condition of the traffic participant in the right lane and successfully executes the *Right-lane change maneuver* toward the road shoulder. Initially, the front TTC drops below the safety threshold, prompting deceleration at -4 m/s^2 from $T = 0$ to 2.12 s. The system continuously evaluates the surrounding traffic, particularly the right-lane rear object, whose TTC and THW gradually improve. At $T = 7.54 \text{ s}$, when both TTC and THW exceed their thresholds, the first lane-change maneuver is initiated, enabling the ego vehicle to safely merge into the adjacent right lane. A second lane change occurs at $T = 12.06 \text{ s}$, allowing the vehicle to enter the road shoulder. Throughout the maneuver, safe relative distances are maintained, and the ego vehicle comes to a complete stop within the shoulder, demonstrating the system's ability to achieve an MRC despite partial sensor failure.

4.3. Discussion

The simulation results across all three scenarios demonstrate that the proposed MRM strategy effectively mitigates the risks associated with potential hazardous events and reduces collision risks, thereby ensuring the safety of both the ego vehicle and surrounding traffic participants. In Scenario A, the ADS regulates deceleration to balance rear-end collision risk and potential forward hazards under front perception sensor failure. In Scenario B, it prioritizes maintaining a safe distance to the front vehicle and, when feasible, maintains its speed to mitigate collision risks arising from potential hazardous events associated with rear perception sensor failure. In Scenario C, the ADS adapts both longitudinal and lateral control to safely perform a rightward lane change and stop on the road shoulder under left-side perception sensor failure.

In Scenario A, the MRM strategy prioritized mitigating hazards in the front blind area by stopping before the virtual object representing undetectable threats. As shown in Figure 11, the simulation confirmed that this approach ensures safe longitudinal control under nominal conditions. However, if the rear vehicle is closer (e.g., $<50 \text{ m}$), traveling faster, or has a longer driver reaction time, the ego vehicle may face an increased rear-end collision risk. These observations highlight a critical tradeoff between mitigating potential hazards from virtual objects and addressing actual rear-vehicle threats, particularly during *Emergency in-lane maneuver* and *Emergency straight maneuver*. Traffic liability considerations are incorporated into the proposed MRM strategy. In Scenario B, with a real front vehicle and a rear virtual object, prioritizing the real front-vehicle threat is appropriate to reduce forward collision risk. Moreover, in severe sensor-failure scenarios where both front and rear targets are represented as virtual objects, giving priority to the forward threat remains a reasonable approach. However, in Scenario A, where a front virtual object is generated while a real vehicle is detected behind, decelerating to stop before the virtual object may expose the ego vehicle to a rear-end collision. Decision-making in such complex situations warrants further investigation, particularly to balance collision severity with traffic liability considerations. Through multiple simulation runs in Scenario C, it is observed that the current strategy tends to be conservative when deciding rightward lane changes toward the road shoulder in order to avoid potential collisions with right-lane vehicles. Future work will investigate traffic liability considerations and conduct additional simulations to refine TTC and THW thresholds, aiming to improve the feasibility of rightward lane changes toward the road shoulder while preserving safety.

5. Conclusions

This study proposed an MRM strategy to enhance the safety of ADSs and surrounding traffic during MRM execution by effectively leveraging the remaining functional sensors under multiple sensor-failure conditions. A HAZOP analysis based on an ADS behavior model was conducted to systematically identify potential hazardous events and categorize them into three hazard types, forming the basis of the proposed decision-making framework. The proposed strategy incorporates sensor-failure awareness through object data derivation and virtual object generation and supports real-time MRM decision-making using TTC- and THW-based risk assessments. Seven MRM action types were defined to adapt MRM behavior to different sensor-failure conditions and surrounding traffic situations. The strategy was implemented in a CARLA–MATLAB co-simulation environment and evaluated in three representative highway scenarios involving front, rear, and lateral perception sensor failures. The simulation results demonstrate that the proposed approach can dynamically adapt MRM behavior to diverse sensor-failure conditions while maintaining safety for both the ego vehicle and the surrounding traffic participants.

Several directions for future work are discussed. First, this study focuses on Level 3 and Level 4 ADSs, assuming the presence of a driver or passengers and addressing safety from a human-centric standpoint. In contrast, Level 5 ADSs may operate without occupants, which implies different safety tolerance requirements. Future research will adapt the proposed MRM strategy to Level 5 ADSs by redefining safety tolerance assumptions and updating the decision-making model accordingly. Second, while the current HAZOP analysis considers complete sensor failure as a conservative baseline, future research will incorporate additional HAZOP guide words to analyze partial sensor failures, such as delayed or degraded sensor responses. Third, ablation studies and sensitivity analyses will be conducted to further improve the proposed strategy, for example, by raising the feasibility of rightward lane changes toward the road shoulder while preserving safety, as indicated by the simulation observations, and by supporting more balanced decision-making by integrating responsibility attribution and hazard severity assessments.

Author Contributions: Conceptualization, J.T. and C.Y. and H.N.; methodology, J.T.; software, J.T.; validation, J.T.; formal analysis, J.T.; investigation, J.T.; resources, H.N.; data curation, C.Y.; writing—original draft preparation, J.T.; writing—review and editing, J.T. and H.N.; visualization, J.T.; supervision, H.N.; project administration, J.T.; funding acquisition, H.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available from the corresponding author upon reasonable request.

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

References

1. SAE International. *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* (SAE J3016); SAE International: Warrendale, PA, USA, 2021.
2. ISO 26262; Road Vehicles—Functional Safety. 2nd ed. International Organization for Standardization: Geneva, Switzerland, 2018.
3. Safety First for Automated Driving Consortium. *Safety First for Automated Driving*; Technical Report; UNECE: Geneva, Switzerland, 2019.
4. United Nations. *Uniform Provisions Concerning the Approval of Vehicles with Regard to Automated Lane Keeping Systems*; ECE/TRANS/WP.29/2020/81; Economic Commission for Europe: Geneva, Switzerland, 2020.
5. European Commission. Commission Implementing Regulation (EU) 2022/1426 on Automated Driving Systems (ADS). In *Official Journal of the European Union*; European Commission: Brussels, Belgium, 2022.

6. ISO 23793-1:2024; Intelligent Transport Systems—Minimal Risk Manoeuvre (MRM) for Automated Driving—Part 1: Framework, Straight-Stop and In-Lane Stop. International Organization for Standardization: Geneva, Switzerland, 2024.
7. Gyllenhammar, M.; Brännström, M.; Johansson, R.; Sandblom, F.; Ursing, S.; Warg, F. Minimal risk condition for safety assurance of automated driving systems. In Proceedings of the CARS: 6th International Workshop on Critical Automotive Applications: Robustness & Safety, Virtual, 13 September 2021.
8. Balakrishnan, K. *Functional Safety Concept of “Minimum Risk Maneuver” in Conditional Driving Automation (Level 3) Vehicles*; SAE Technical Paper 2022-28-0301; SAE International: Warrendale, PA, USA, 2022. [[CrossRef](#)]
9. Schindler, J.; Herbig, D.L.; Lau, M.; Oehl, M. Communicating Issues in Automated Driving to Surrounding Traffic—How should an Automated Vehicle Communicate a Minimum Risk Maneuver via eHMI and/or dHMI? In *HCI International 2020—Late Breaking Posters*; Stephanidis, C., Antona, M., Ntoa, S., Eds.; Communications in Computer and Information Science; Springer: Cham, Switzerland, 2020; Volume 1294, pp. 619–626. [[CrossRef](#)]
10. Karakaya, B.; Bengler, K. Minimal Risk Maneuvers of Automated Vehicles: Effects of a Contact Analog Head-Up Display Supporting Driver Decisions and Actions in Transition Phases. *Safety* **2023**, *9*, 7. [[CrossRef](#)]
11. Nagayoshi, M.; Watanuki, K.; Kaede, K.; Osawa, Y. Effects of Different Alarm Methods of Minimum Risk Maneuver on Drivers of Following Vehicles in Automatic Driving. In *Proceedings of the Affective and Pleasurable Design, AHFE International Conference, San Francisco, CA, USA, 20–24 July 2023*; Fukuda, S., Ed.; AHFE Open Access; AHFE International: Honolulu, HI, USA, 2023; Volume 71. [[CrossRef](#)]
12. Hub, F.; Hess, S.; Lau, M.; Wilbrink, M.; Oehl, M. Promoting trust in HAVs of following manual drivers through implicit and explicit communication during minimal risk maneuvers. *Front. Comput. Sci.* **2023**, *5*, 1154476. [[CrossRef](#)]
13. Tong, K.; Solmaz, S.; Horn, M. A Search-based Motion Planner Utilizing a Monitoring Functionality for Initiating Minimal Risk Maneuvers. In Proceedings of the 2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC), Macau, China, 8–12 October 2022; pp. 4048–4055. [[CrossRef](#)]
14. Vu, V.; Warg, F.; Thorsén, A.; Ursing, S.; Sunnerstam, F.; Holler, J.; Bergenhem, C.; Cosmin, I. Minimal Risk Manoeuvre Strategies for Cooperative and Collaborative Automated Vehicles. In Proceedings of the 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Porto, Portugal, 27–30 June 2023; pp. 116–123. [[CrossRef](#)]
15. Svensson, L.; Masson, L.; Mohan, N.; Ward, E.; Brenden, A.P.; Feng, L.; Törngren, M. Safe Stop Trajectory Planning for Highly Automated Vehicles: An Optimal Control Problem Formulation. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV), Changshu, China, 26–30 June 2018; pp. 517–522. [[CrossRef](#)]
16. Xue, W.; Yang, B.; Kaizuka, T.; Nakano, K. A fallback approach for an automated vehicle encountering sensor failure in monitoring environment. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV), Changshu, China, 26–30 June 2018; pp. 1807–1812. [[CrossRef](#)]
17. Wang, L.; Wu, Z.; Li, J.; Stiller, C. Real-Time Safe Stop Trajectory Planning via Multidimensional Hybrid A*-Algorithm. In Proceedings of the 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), Rhodes, Greece, 20–23 September 2020; pp. 1–7. [[CrossRef](#)]
18. Thorn, E. *A Framework for Automated Driving System Testable Cases and Scenarios*; National Highway Traffic Safety Administration (NHTSA): Washington, DC, USA, 2018.
19. International Council on Systems Engineering (INCOSE). *Systems Engineering Handbook: A Guide for System Life Cycle Process and Activities*, 4th ed.; INCOSE: Washington, DC, USA, 2015.
20. Friedenthal, S.; Moore, A.; Steiner, R. *A Practical Guide to SysML: The System Modeling Language*, 3rd ed.; Morgan Kaufmann/OMG Press: Waltham, MA, USA, 2014.
21. Lovric, T.; Schneider-Scheyer, M.; Sarkic, S. *SysML as Backbone for Engineering and Safety—Practical Experience with TRW Braking ECU*; SAE Technical Paper 2014-01-0212; SAE International: Warrendale, PA, USA, 2014. [[CrossRef](#)]
22. Jahromi, B.S.; Tulabandhula, T.; Cetin, S. Real-Time Hybrid Multi-Sensor Fusion Framework for Perception in Autonomous Vehicles. *Sensors* **2019**, *19*, 4357. [[CrossRef](#)]
23. Matos, F.; Bernardino, J.; Durães, J.; Cunha, J. A Survey on Sensor Failures in Autonomous Vehicles: Challenges and Solutions. *Sensors* **2024**, *24*, 5108. [[CrossRef](#)] [[PubMed](#)]
24. Vargas, J.; Alsweiss, S.; Toker, O.; Razdan, R.; Santos, J. An Overview of Autonomous Vehicles Sensors and Their Vulnerability to Weather Conditions. *Sensors* **2021**, *21*, 5397. [[CrossRef](#)] [[PubMed](#)]
25. Bogdoll, D.; Uhlemeyer, S.; Kowol, K.; Zöllner, J.M. Perception Datasets for Anomaly Detection in Autonomous Driving: A Survey. In Proceedings of the 2023 IEEE Intelligent Vehicles Symposium (IV), Anchorage, AK, USA, 4–7 June 2023; pp. 1–8. [[CrossRef](#)]
26. Yeong, D.J.; Velasco-Hernandez, G.; Barry, J.; Walsh, J. Sensor and Sensor Fusion Technology in Autonomous Vehicles: A Review. *Sensors* **2021**, *21*, 2140. [[CrossRef](#)] [[PubMed](#)]
27. Neupane, S.R.; Sun, W. Advanced Data Classification Framework for Enhancing Cyber Security in Autonomous Vehicles. *Automation* **2025**, *6*, 5. [[CrossRef](#)]

28. International Electrotechnical Commission. *IEC 61882:2016–Hazard and Operability Studies (HAZOP Studies)—Application Guide*; IEC: Geneva, Switzerland, 2016.
29. Zhou, W.; Wang, X. Calibrating and Comparing Autonomous Braking Systems in Motorized-to-Non-Motorized-Vehicle Conflict Scenarios. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 20636–20651. [[CrossRef](#)]
30. Jiang, R.; Zhu, S.; Chang, H.; Wu, J.; Ding, N.; Liu, B.; Qiu, J. Determining an Improved Traffic Conflict Indicator for Highway Safety Estimation Based on Vehicle Trajectory Data. *Sustainability* **2021**, *13*, 9278. [[CrossRef](#)]
31. Liu, K.; Ma, J.; Lai, E.M.-K. Dynamic Car-Following Model With Jerk Suppression for Highway Autonomous Driving. *IEEE Access* **2025**, *13*, 23111–23119. [[CrossRef](#)]
32. MathWorks. Call Python Libraries from MATLAB. Available online: <https://www.mathworks.com/help/matlab/call-python-libraries.html> (accessed on 10 June 2024).
33. CARLA Simulator Team. CARLA: An Open-Source Simulator for Autonomous Driving. Available online: <https://github.com/carla-simulator/carla> (accessed on 10 June 2024).
34. CARLA Simulator Team. CARLA Python API Documentation. Available online: https://carla.readthedocs.io/en/latest/python_api/ (accessed on 10 June 2024).

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.