Risk Monitoring and Mitigation for Automated Vehicles: A Model Predictive Control Perspective

1st Kailin Tong
Control Systems Group (Dept.-E)
Virtual Vehicle Research GmbH
Graz, 8010 Austria
kailin.tong@v2c2.at

2nd Fengwei Guo
Vehicle Safety Institute
Graz University of Technology
Graz, 8010 Austria
fengwei.guo@student.tugraz.at

3rd Selim Solmaz
Control Systems Group (Dept.-E)
Virtual Vehicle Research GmbH
Graz, 8010 Austria
selim.solmaz@v2c2.at

4th Martin Steinberger
Institute of Automation and Control
Graz University of Technology
Graz, 8010 Austria
martin.steinberger@tugraz.at

5th Martin Horn
Institute of Automation and Control
Graz University of Technology
Graz, 8010 Austria
martin.horn@tugraz.at

2023 IEEE International Automated Vehicle Validation Conference (IAVVC) | 979-8-3503-2253-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/IAVVC57316.2023.10328124

***Abstract*—Despite recent advances in algorithms and technology, self-driving vehicles are still susceptible to errors that can have severe consequences. As a result, effective risk monitoring and mitigation measures for autonomous driving systems are in high demand. To overcome this issue, several specifications and standards have been developed. However, a theoretical framework for dealing with autonomous vehicle hazards has rarely been presented. This study suggests a risk modeling method inspired by ideas from control theory and introduces a Model Predictive Control (MPC) Framework to deal with risks in general. Two application examples are presented. The first example shows how MPC parameters may affect the aggressiveness of the response. In the second example, our proposed risk monitoring and mitigation module is integrated into a vision-based Adaptive Cruise Control (ACC) system. Simulation results indicate a significant improvement in collision avoidance rate (from 0% to 47% in edge scenarios) during the Euro NCAP ACC Car-to-Car tests with a stationary target, which demonstrates the utility of our approach for addressing various types of hazards faced by autonomous vehicles.**

***Index Terms*—automated vehicles, model predictive control, risk monitoring, risk mitigation, functional safety**

I. Introduction

In the automotive industry, automated driving technology is expected to lead to a paradigm shift in transportation systems, introduce new business models and improve user experience. Given the current momentum, it can be assumed that (highly) automated vehicles will advance continuously. However, despite tremendous advances in sensor technology, high-performance computing, deep learning, computer vision, data fusion techniques, and other systems technologies, bringing a fully automated vehicle (AV) capable of driving unattended in complex and various scenarios is a long-term effort. To be accepted by drivers and other stakeholders, automated vehicles must be reliable and much safer than current cars. However, automated driving technology also introduces new challenges. New perception algorithms, including machine learning and sensor fusion, exhibit complex, non-deterministic, and potentially unpredictable behaviors. Besides, automated vehicles rely on multiple sensors and computation units, so hardware imperfections or failures critically impact planning and decision-making. Those risk factors must be taken into account and adequately handled.

While automated driving technology has the potential to alter the way we travel, it also raises serious safety issues. Automated vehicles must conform to various safety requirements to protect the safety of passengers and other road users. The capacity to monitor safety parameters in real-time is an essential component of these standards since it allows for the instant discovery of possible safety dangers and the opportunity to take remedial action before accidents occur. Runtime monitoring of safety parameters entails evaluating several elements of the vehicle's performance during its operation. In addition to monitoring the vehicle's position and speed, it is necessary to check additional safety parameters during runtime. Risk monitoring employs a combination of hardware and software components to monitor key safety factors efficiently. If a hazard is detected, a risk mitigation module is activated and alters the vehicle's behavior to avoid critical consequences.

Overall, a runtime Risk Monitoring and Mitigation (RMM) module is and should be an essential part of automated driving technology. Automated driving systems can help prevent accidents and maintain the safety of all road users by continually monitoring the vehicle's position, speed, and other safety data. As technology advances, these safety criteria are expected to become even more standardized, boosting the safety of autonomous cars on our roads.

Risk monitoring and assessment aims to evaluate the severity of a hazard event and provide correspondent mitigation control actions. The risk from the hazardous event can be classified into internal risk (caused by vehicle) and external risk (caused by the environment). For example, internal risks can be malfunctions, faults, or failures of the perception system. In contrast, external risks are related to extreme weather and light conditions for the perception systems [1]. Quite a few researchers attempt to contribute to risk assessment and mitigation framework. The risk assessment methodologies can be classified into process-driven, model-based, probability and model-based, AI-based, and cooperative mode-based methodology [1]. One notable work for the model-based approach is Responsibility Sensitive Safety (RSS). RSS is a formal, mathematical model for AV safety intended to be used as a safety concept for AV behaviour planning [2]. Differently, Xiao et al. [3] proposed event-agnostic metrics and demonstrated a configurable framework for detection and dataset annotation. Another interesting direction but with a different focus is risk-aware motion planning and control. Risk can be modelled as collision probability, and Model Predictive Control (MPC) is a popular approach for minimizing risk. For example, an optimal overtaking problem considering predicted motion uncertainties is formulated as a non-linear optimization problem in [4]. In [5], the risk is modelled as the probability of violating the safety specifications. By combining the risk measure, their trajectory planner can plan minimal-risk trajectories while quantifying trade-offs between risk and driving progress.

Numerous safety standards and specifications have been proposed for various risk assessment methodologies for automated vehicles. Although considerable research has been conducted on reducing collision risk, there is a lack of reported studies on a comprehensive framework for handling (external and internal) hazards from different sources. This paper aims to bridge functional safety and control theory concepts by incorporating definitions such as risk mitigation stability, hazard controllability, and hazard observability. Building upon this foundation, we present a novel Model Predictive Control (MPC) framework that addresses the handling of hazards. The effectiveness of the framework is demonstrated through two representative examples in simulation. Extending the proposed framework to monitor and mitigate various hazards in more diverse scenarios is achievable.

This paper is structured as follows: Section 2 discusses the theoretical background of the research. The Model Predictive Control framework is presented in Section 3. Section 4 discusses the experimental examples. Finally, the conclusion and outlook are shown in Section 5.

II. Preliminaries and Background

A. Problem Formulation

For the system dynamics, we use the common state transition model.

$$\mathbf{x}_{k+1} = F(\mathbf{x}_k, \mathbf{u}_k) \tag{1}$$

where $\mathbf{x}_k \in \mathbb{R}^n$ is a state vector, $\mathbf{u_k} \in \mathbb{R}^m$ is the control input.

To evaluate the risk of a hazard, we use the most common definition of risk: risk is the probability times severity [1]. We first define the severity s_k of a hazard at time step k. Its severity model is given by

$$s_{k+1} = S(\mathbf{x}_{k+1}, s_k) \tag{2}$$

We denote a hazard as H for the Automated Driving System. The state is either h, meaning occurrence of the hazard, or $\bar{h}$, meaning no occurrence of the hazard. The observation monitoring the hazard at the k-th step is denoted as $\mathbf{z}_k$. We define the probability of hazard conditioned on observations as $p_k = p(h|\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_k)$. Finally, we have the risk model:

$$r_k = s_k \cdot p_k \tag{3}$$

B. Definitions

Definition 1 (Safe Set) *The state vector $\mathbf{x}_k$ in a bounded space $\mathbb{X} \subset \mathbb{R}^n$ and the hazard-related observation $\mathbf{z_k}$ in a bounded space $\mathbb{Z} \subset \mathbb{R}^m$ span a space $\chi \subset \mathbb{R}^{n+m}$. α is an acceptable risk level, which defines the boundary of the Safe Set $\chi^\alpha \subset \chi$. The Safe Set represents the normal operation of the Automated Driving System (ADS).*

The risk for a hazard is monitored during the operation of the ADS. As the standard ISO 26262 requires, a risk mitigation system keeps the AV safe if a hazard occurs.

Definition 2 (Stability of Risk Mitigation): *The risk of a hazard can be brought back to the Safe Set in [t_0, t_{f1}] if the risk is greater than an acceptable risk level α, as shown in Fig. 1 .*

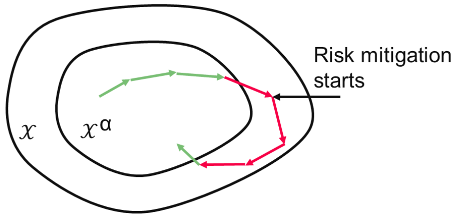


Fig. 1: Illustration of stability of risk mitigation.

Definition 3 (Controllability of a Hazard): *If a hazard occurs, there exists a vector of $\mathbf{u}_k$ that can bring the risk of a hazard to the Safe Set in [t_0, t_{f2}], and the hazard is controllable. t_{f2} is the deadline for tolerating the existence of a hazard.*

Definition 4 (Observability of a Hazard): *If there exists a vector of Observations $\mathbf{z}_k$ measured by the ADS which can estimate the probability of a hazard in [t_0, t_{f3}], the hazard is observable. t_{f3} is the deadline for detecting the existence of a hazard.*

C. System Architecture

The SENSE-PLAN-ACT Paradigm is commonly used in the ADS [6]. SENSE and PLAN require a large amount of computation power, while ACT requires fewer computation resources but higher reliability. This kind of distribution of resources has been applied in some recent commercialized products with Advanced Driver Assistance Systems (ADAS).

Fig. 2 shows our proposed system architecture for our AD demonstrator. We implement the risk monitoring and risk mitigation software in the simulation and will further apply it in the AD demonstrator.

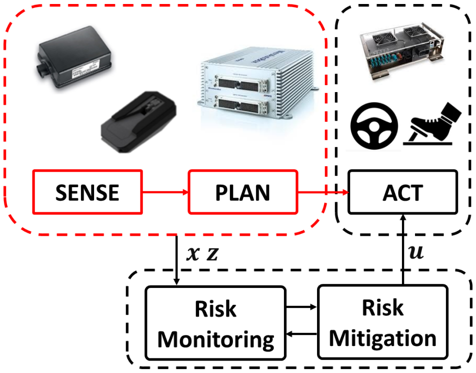


Fig. 2: Illustration of the proposed architecture for our AD demonstrator. The dashed block denotes hardware, while the solid block denotes software. We monitor the hardware and software of SENSE and PLAN, which are marked with red color. The Risk Monitoring and Mitigation (RMM) Module on the lower side is an additional software block to monitor and mitigate the risk.

III. Model Predictive Control Framework

The proposed RMM module monitors the risk online and triggers risk mitigation. For any nominal planner, the Risk Mitigation Module is a supervisory planner that enforces the risk to return to χ^α if a hazard happens (its risk is higher than the acceptable level α). To simplify our formulation, we let $\mathbf{u}_k \in R$ and $\bar{\mathbf{u}}_k$ be the control until the end of the prediction horizon N_p. Motivated by Safety Barrier Functions [7], we have the following quadratic programming (QP) problem with hard constraints:

$$\begin{aligned} \mathbf{u}^* = &\arg\min_{\bar{\mathbf{u}}_\mathbf{k}\in\mathbb{U}} \quad ||\bar{\mathbf{u}}_k - \mathbf{u}_0||^2_\mathbf{Q} \\ & s.t. \quad r_i \le \alpha, \quad k+N_d \le i \le k+N_p \end{aligned} \tag{4}$$

where $\mathbf{u}_0$ is a vector of length N_p where each element is the output from a nominal planner at time step k. N_d is the deadline for bringing the risk less than α. $\bar{\mathbf{u}}_k = [u_k, u_{k+1}, \dots, u_{k+N_c}, \dots, u_{k+N_p-1}]^T$, where N_c is the control horizon. If N_c is smaller than N_p, after $k+N_c$ step, the control is same as u_{k+N_c}.

The weighting matrix $\mathbf{Q}$ is defined as:

$$\mathbf{Q} = \begin{bmatrix} \lambda & 0 & \dots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \lambda^{Np-1} & 0 \\ 0 & \dots & 0 & \lambda^{N_p} \end{bmatrix}$$

where λ is a factor in $[0,1]$

The matrix Q smooths the transition from a nominal state to an evasive maneuver (like a hard brake) but finally applies more aggressive emergency actions. This also corresponds to the requirement of ISO 26262, as there is the transition to emergency operation instead of directly applying emergency operation.

We predict the future evolution of the risk and assume that the probability of the hazard remains constant. So we have

$$\begin{aligned} r_{k+1} =& s_{k+1} \cdot p_{k+1} \\ =& S(F(\mathbf{x}_k, \mathbf{u}_k), s_k) \cdot p_k \end{aligned} \tag{5}$$

We have introduced our framework. In the next section, we provide two examples to showcase how our framework can be applied in handling hazards.

IV. Experimental Examples

In this section, we provide two experimental examples to demonstrate the benefits of our proposed framework for reducing risks.

A. Hardware Hazard: Camera Offline

Considering an automated vehicle is driving in a suburban area with ACC (Adaptive Cruise Control), we envisage a critical hazard where the camera is offline, and the vehicle has no redundant sensor configuration. Hence the ACC function cannot continue.

We only consider the longitudinal dynamics and use a single integrator model for the hazard. So the state transition model is

$$v_{k+1} = v_k + \Delta T u_k \tag{6}$$

where v_k denotes velocity, u_k denotes acceleration and ΔT is the time step size. The severity of this hazard relies on ego velocity as we lose perception capability. Hence we define a simple severity model

$$s_k = (v_k - v_s)^2. \tag{7}$$

The stable velocity denoted as v_s, is determined by specific regulations: in urban driving, it corresponds to a complete stop, while on the highway, it is set at $80km/h$ under typical driving circumstances.

Commonly, the camera hardware provides a safety flag to show whether it operates normally or not. We denote this safety flag at time step k as z_k. We assume that the observation follows the Markov assumption at each time step with the following probability model

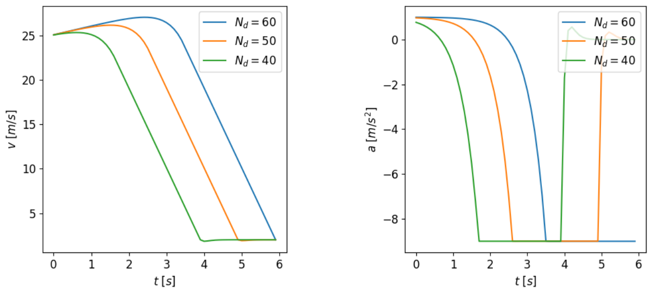
$$p_k = \begin{cases} 1, & \text{if } z_k = 1 \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

Hence we can formulate the optimization problem.

$$\begin{aligned} \mathbf{u}^* = &\arg\min_{\bar{\mathbf{u}}_\mathbf{k}} \quad ||\bar{\mathbf{u}}_\mathbf{k} - \mathbf{u_0}||^2_\mathbf{Q} \\ s.t. \quad & -\sqrt{\alpha} + v_s - v_k \le \sum_{j=0}^{i-1} \Delta T u_{k+j} \le \sqrt{\alpha} + v_s - v_k, \\ & i = N_d, N_{d+1}, \dots, N_p, \\ & 0 \le v_{k+i} \le v_{max}, i = 1, 2, \dots, N_p, \\ & u_i \in [u_{min}, u_{max}], i = k, k+1, \dots, k+N_p-1, \end{aligned} \tag{9}$$

where $\mathbf{\bar{u}_k} = [u_k, u_{k+1}, \dots, u_{k+N_c}, \dots, u_{k+N_p-1}]^T . \mathbf{\bar{u}_0} = [a_0, a_0, \dots, a_0]^T$, where a_0 is the output of the ACC function before a hazard is detected. v_s is a stable velocity.

We have the following parameters for the suburban driving scenario. $v_s = 0, \Delta T = 0.1s, x_0 = 25m/s, u_0 = 1m/s^2, u_{max} = 6m/s^2, u_{min} = -9m/s^2$. We define $\alpha = 1.0$ and $x_s = 1m/s$ and let $N_p = N_c = 60$, $v_{max} = 100km/h$. We experimented with different N_d (60, 50, 40). The factor λ in matrix $\mathbf{Q}$ is 0.8.



(a) Velocity.

(b) Acceleration.

Fig. 3: Illustration of velocity and acceleration with different N_d.

Fig. 3 illustrates the velocity and acceleration regarding different N_d when the camera is offline. We can see that a small N_d leads to a quicker deceleration, and the ego vehicle is brought to a safe set earlier. However, this will cause a shorter transition time. If the fault was recovered during the transition time, such a quick reaction would not be necessary and would result in the discomfort of passengers.

B. Software Hazard: Error of Perception Algorithm

ADS faces significant challenges in accurately perceiving the surrounding environment, including identifying and continuously tracking surrounding objects. A failure of the perception module often results in severe traffic accidents [8]. In this section, we demonstrate the necessity of Risk Monitoring and Risk Mitigation by presenting an example of how it improves the safety of the vision-based ACC system through risk assessment and control.

1) Confirmation problem in object tracking: The objective of risk monitoring, in this case, is to verify the correct functioning of object tracking. When the detection is passed to a multi-object tracking module, an attempt is made to match the input detection to existing tracks. If the tracks cannot be matched, a confirmation process is applied based on the defined confirmation threshold. A commonly used method is to check whether the new detection has been detected at least a certain number of times in the last several updates [9]. The threshold should be carefully chosen to achieve an optimal balance between computational cost and the possibility of both false positives and false negatives.

2) Example hazardous scenarios:

- *Vision-based ACC:* We implemented a vision-based ACC based on Autoware.AI [10]. The system consists of four main modules: an object detection module based on the darknet module in Autoware.AI, a multi-object tracking algorithm based on Global Nearest Neighbor, the ACC strategy proposed in the paper of Rahman et al. [11], and a lower-level vehicle control module based on pure pursuit and PID control.
- *External scenarios:* In 2020, The European New Car Assessment Programme (Euro NCAP) introduced the Test and Assessment Protocol for highway assist systems [12], which included testing scenarios for the performance of Adaptive Cruise Control (ACC). We conducted tests on the vision-based ACC system in the prescribed straight road scenarios, as listed in Table I, and successfully avoided collisions in all scenarios except for the Car-to-Car Rear Stationary (CCRs) scenario when the ego speed exceeded 100 km/h. A white Toyota Prius similar to the one used in Euro NCAP tests (as shown in Fig 4) was used during testing. Subsequently, different types of target vehicles provided by Carla simulator [13] were used to replace the white car for testing. We observed that certain types of target vehicles, like a light truck ”CarlaCola” with the original color set by Carla Simulator (as shown in Fig 4), posed significant challenges to the perception module of the vision-based ACC system, as they could not be identified successfully. These scenarios are considered hazardous scenarios for the vision-based ACC system. We propose a risk monitoring and mitigation method that will be integrated with the vision-based ACC system and retested in these hazardous scenarios to evaluate its effectiveness.

TABLE I: Euro NCAP ACC Car-to-Car test scenarios with Stationary and Moving Target (straight roads) [12]

Scenarios	**Vehicle under Test**	**Global Vehicle Target**
Car-to-Car Rear Stationary (CCRs)	70, 80, 90, 100, 110, 120, 130 km/h	0 km/h
Car-to-Car Rear Moving (CCRm)	80, 90, 100, 110, 120, 130 km/h	20 km/h
	80, 90, 100, 110, 120, 130 km/h	60 km/h

3) Perception algorithm risk monitoring and mitigation method: To address the potential risks associated with the perceived limitations of vision-based ACC, a module, as depicted in Fig. 5, has been developed and incorporated into the ACC. In addition to the detection-confirmation-tracking-strategy-control pipeline, objects that are detected but not confirmed and tracked are separately listed for monitoring in parallel. If there are objects judged to be approximately the same object, based on their color, aspect ratio, and position

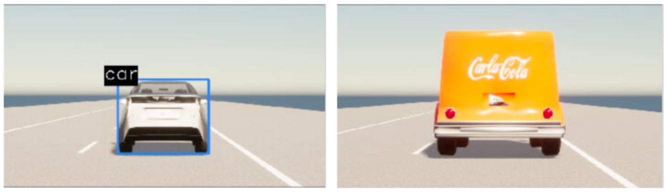


Fig. 4: Ground Vehicle Targets: Toyota Prius (left) and CarlaCola (right). The perception system can track the Toyota Prius precisely. However, it occasionally loses track of the CarlaCola.

in the image, in at least four out of the past 20 frames and the object has not been tracked, then the perception function is deemed hazardous. If a hazard is detected, the vehicle is controlled using the risk mitigation method described below (indicated by the red line in Fig. 5); otherwise, a standard ACC logic is used for control (indicated by the green line in Fig. 5). In hazardous situations, the vehicle under test is controlled by the model predictive controller described below to mitigate the risk.

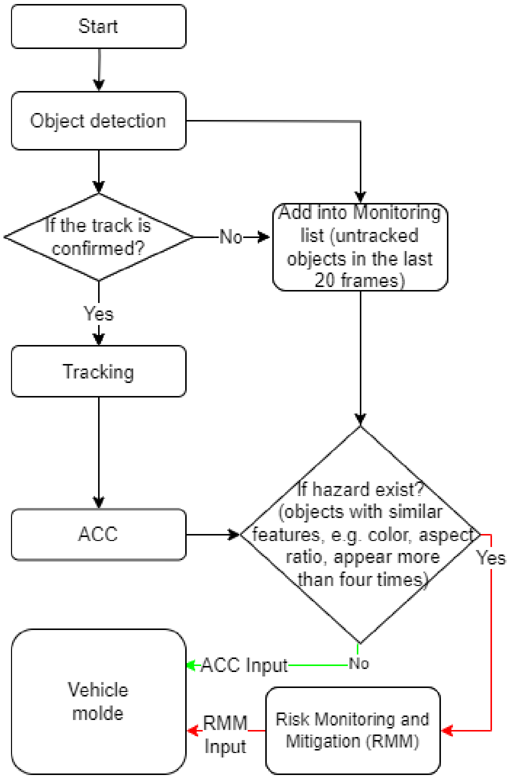

Start
Object detection
If the track is confirmed?
No
Add into Monitoring list (untracked objects in the last 20 frames)
Yes
Tracking
ACC
If hazard exist? (objects with similar features, e.g. color, aspect ratio, appear more than four times)
Yes
No
ACC Input
Vehicle molde
RMM Input
Risk Monitoring and Mitigation (RMM)

Fig. 5: Risk Monitoring and Mitigation for Vision-based ACC

In the model predictive controller for risk mitigation, a double integrator model is used to predict the longitudinal kinematics of the vehicle under test.

$$\ddot{d} = u \tag{10}$$

where u is the longitudinal acceleration, and d is the longitudinal distance.

Therefore, we have the following state transition model

$$x_{k+1} = Ax_k + Bu_k, \tag{11}$$

where $x_k = \begin{bmatrix} d_k \\ v_k \end{bmatrix}$, $A = \begin{bmatrix} 1 & \Delta T \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} \frac{1}{2}\Delta T^2 \\ \Delta T \end{bmatrix}$ and

$$y_k = Cx_k, \tag{12}$$

where $C = \begin{bmatrix} 0 & 1 \end{bmatrix}$ and $y_k = v_k$.

Similar to the first example, the severity of this hazard relies on ego velocity as the perception system is unreliable. And a full stop to $v_s = 0$ will bring minimal hazard severity in this scenario. So we let the severity of the perception hazard be the same as the velocity and assume that a full stop is the safe state of the ego vehicle.

$$s_k = v_k \tag{13}$$

We have the following binary probability model for hazard detection:

$$p_k = \begin{cases} 1, & \text{if a perception error is detected} \\ 0, & \text{otherwise} \end{cases} \tag{14}$$

Finally, we obtain the following optimization problem.

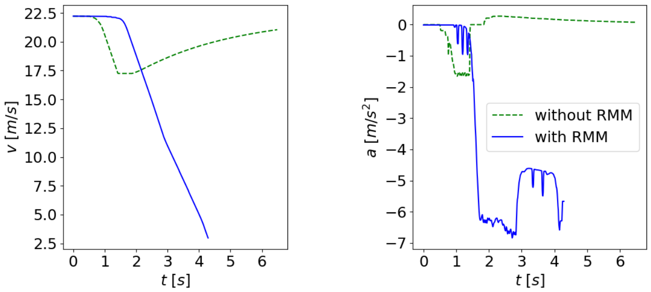
$$\begin{aligned} \mathbf{u}^* = & \arg\min_{\bar{\mathbf{u}}_\mathbf{k}} \quad ||\bar{\mathbf{u}}_\mathbf{k} - \mathbf{u_0}||^2_\mathbf{Q} \\ s.t. \quad & v_{k+i} \leq \alpha, i = N_d, N_{d+1}, \ldots, N_p \\ & 0 \leq v_{k+i} \leq v_{max}, i = 1, \ldots, N_p \\ & u_i \in [u_{min}, u_{max}], i = k, k+1, \ldots, k+N_p-1 \end{aligned} \tag{15}$$

where $\bar{\mathbf{u}}_\mathbf{k} = [u_k, u_{k+1}, \ldots, u_{k+N_c}, \ldots, u_{k+N_p-1}]^T$. $\bar{\mathbf{u}}_0 = [a_0, a_0, \ldots, a_0]^T$, where a_0 is the output of the ACC function. α is the acceptable risk, which is a small threshold $\epsilon > 0$ in this scenario.

N_d is determined as follows. We get the distance d_k and current ego velocity v_k at time step k when the error of the perception algorithm is detected. And the time headway is calculated as d_k/v_k assuming the front vehicle stands still. It is the worst-case time limit to avoid a crash. So N_d is the rounded value of $(d_k/v_k)/\Delta T$. If N_d is larger than N_p, we let $N_d = N_p$.

4) Simulation: Simulations were conducted using the Carla simulator to compare the performance of the vision-based ACC with and without the Risk Monitoring and Mitigation (RMM) module in the scenarios listed in Table I. Except for the Ground Vehicle Target, the simulations replicate the scenarios' definition in the Test Protocol [12]. The ”Carlacola” small truck offered by the Carla Simulator was used as the Ground Vehicle Target, as illustrated in Fig 4. The Carla simulator provides a high-fidelity environment and sensor simulations. The input signal for the vision-based ACC was the raw image signal generated by the RGB camera provided in the Carla Simulator. The multi-body vehicle dynamics model provided in CommonRoad [14] was improved and utilized for the dynamics simulation of the ego car. To ensure accuracy and reliability, each simulation was repeated 10 times.

5) Results: Fig. 6 presents the simulation results of vision-based ACC with and without the RMM module in a hazardous scenario where the ground vehicle target is stationary, and the velocity of the vehicle under test is 80 km/h. When the relative distance between the two vehicles was 90 m, and the ground vehicle target was stationary, the ACC system, without the RMM module, tracked the target and applied appropriate braking. However, the system lost track of the target due to detection hazards, switched to a speed maintenance mode (80 km/h), and accelerated. On the other hand, in the same scenario, the ACC system equipped with the module identified the hazard and controlled the vehicle to reach the lowest risk state by applying the brakes and stopping the ego vehicle.



(a) Velocity

(b) Acceleration

Fig. 6: Illustration of velocity, and acceleration with or without Risk Monitoring and Mitigation (RMM)

Table II summarizes the simulation results and provides the collision avoidance rates of the vision-based ACC system for each test scenario under three different settings. ”70 km/h V.S. 0 km/h” means that the Vehicle Under Test is traveling at 70 km/h, while the ground vehicle target is stationary at a speed of 0 km/h. The ”Original” setting refers to the vision-based ACC system test results without the RMM module in the original Euro NCAP scenarios (where the target vehicle is a white Toyota Prius) that do not result in hazards and are used as a reference in the table. For the hazardous scenarios (where the target vehicle is CarlaCola), it can be observed that introducing the RMM module reduces the risk and increases the average collision avoidance rate from 0% to approximately 47%.

TABLE II: Simulation Results: Collision Avoidance Rate with respect to Euro NCAP ACC Car-to-Car test scenarios with Stationary and Moving Target (straight)

Scenario	**Original**	**Hazardous, with RMM**	**Hazardous, without RMM**
70 km/h V.S. 0 km/h	100%	60%	0%
80 km/h V.S. 0 km/h	100%	70%	0%
90 km/h V.S. 0 km/h	100%	40%	0%
100 km/h V.S. 0 km/h	100%	40%	0%
110 km/h V.S. 0 km/h	0%	0%	0%
120 km/h V.S. 0 km/h	0%	0%	0%
130 km/h V.S. 0 km/h	0%	0%	0%
80 km/h V.S. 20 km/h	100%	70%	0%
90 km/h V.S. 20 km/h	100%	60%	0%
100 km/h V.S. 20 km/h	100%	50%	0%
110 km/h V.S. 20 km/h	100%	50%	0%
120 km/h V.S. 20 km/h	100%	40%	0%
130 km/h V.S. 20 km/h	0%	0%	0%
80 km/h V.S. 60 km/h	100%	80%	0%
90 km/h V.S. 60 km/h	100%	70%	0%
100 km/h V.S. 60 km/h	100%	80%	0%
110 km/h V.S. 60 km/h	100%	70%	0%
120 km/h V.S. 60 km/h	100%	60%	0%
130 km/h V.S. 60 km/h	100%	50%	0%
Average	78.94%	46.84%	0%

V. Conclusion and Outlook

Functional safety has been a critical topic for ADS. Many standards and specifications have emerged for the safety of automated driving, but theoretical fundamentals for handling hazards have been little investigated. This paper formally defines the stability of risk mitigation and the Controllability and Observability of a hazard. Based on these, an MPC framework for handling general hazards was proposed. To validate our concept, we implemented two examples. The first example is the hardware hazard of a camera offline. By tuning the parameters of the MPC framework, we can control how aggressive the risk mitigation is. We integrate our RMM module into a vision-based ACC system in the second example. A hazard occurs due to the incapability of detecting the ”Carlacola” small truck, and a collision frequently happens in the Euro NCAP ACC Car-to-Car test scenarios with the ”Carlacola” small truck as a stationary target. With our proposed RMM module, some accidents in the experiments can be avoided, and the average collision avoidance rate is increased from 0% to approximately 47%.

In the future, we plan to demonstrate the proposed framework with our demonstrator for more general hazards.

Acknowledgment

The publication was written at Virtual Vehicle Research GmbH within the scope of the EU project ArchitectECA2030 and under grant agreement No 877539, and ESRIUM Project, which has received funding from the European Union Agency for the Space Programme under grant agreement No 101004181. The project is co-funded by grants from Germany, Netherlands, Czech Republic, Austria, Norway and - Electronic Component Systems for European Leadership Joint Undertaking (ECSEL JU). The authors would like to further acknowledge the financial support within COMET Competence Centers for Excellent Technologies from the Austrian Federal Ministry for Climate Action, the Austrian Federal Ministry for Labour and Economy, the Province of Styria (Dept. 12) and the Styrian Business Promotion Agency (SFG). The Austrian Research Promotion Agency (FFG) has been authorised for the programme management. The content of this paper reflects only the authors’ view. Neither the European Commission nor the EUSPA is responsible for any use that may be made of the information it contains.

References

[1] W. M. D. Chia, S. L. Keoh, C. Goh, and C. Johnson, “Risk assessment methodologies for autonomous driving: A survey,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–17, 2022.

[2] F. Oboril and K.-U. Scholl, “Risk-aware safety layer for av behavior planning,” in *2020 IEEE Intelligent Vehicles Symposium (IV)*, 2020, pp. 1922–1928.

[3] D. Xiao, W. G. Geiger, H. Y. Yatbaz, M. Dianati, and R. Woodman, “Detecting hazardous events: A framework for automated vehicle safety systems,” in *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)*, 2022, pp. 641–646.

[4] Y. Gao, F. J. Jiang, L. Xie, and K. H. Johansson, “Risk-aware optimal control for automated overtaking with safety guarantees,” *IEEE Transactions on Control Systems Technology*, vol. 30, no. 4, pp. 1460–1472, 2022.

[5] T. Nyberg, C. Pek, L. Dal Col, C. Norén, and J. Tumova, “Risk-aware motion planning for autonomous vehicles with safety specifications,” in *2021 IEEE Intelligent Vehicles Symposium (IV)*, 2021, pp. 1016–1023.

[6] S. M. LaValle, *Planning algorithms*. Cambridge university press, 2006.

[7] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, “Control barrier function based quadratic programs for safety critical systems,” *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2016.

[8] Y. Tian, K. Pei, S. Jana, and B. Ray, “Deeptest: Automated testing of deep-neural-network-driven autonomous cars,” in *Proceedings of the 40th international conference on software engineering*, 2018, pp. 303–314.

[9] MathWorks, “Introduction to using the global nearest neighbor tracker,” https://nl.mathworks.com/help/fusion/ug/introduction-to-using-the-global-nearest-neighbor-tracker.html, Accessed on May 14, 2023.

[10] S. Kato, E. Takeuchi, Y. Ishiguro, Y. Ninomiya, K. Takeda, and T. Hamada, “An open approach to autonomous vehicles,” *IEEE Micro*, vol. 35, no. 6, pp. 60–68, 2015.

[11] R. Rahman, S. Hasan, and M. H. Zaki, “Towards reducing the number of crashes during hurricane evacuation: Assessing the potential safety impact of adaptive cruise control systems,” *Transportation research part C: emerging technologies*, vol. 128, p. 103188, 2021.

[12] Euro NCAP, “Euro NCAP Assisted Driving - Highway Assist Systems Test and Assessment Protocol v1.0,” Euro NCAP, Tech. Rep., September 2020. [Online]. Available: https://cdn.euroncap.com/media/58813/euro-ncap-ad-test-and-assessment-protocol-v10.pdf

[13] A. Dosovitskiy, G. Ros, F. Codevilla, A. Lopez, and V. Koltun, “Carla: An open urban driving simulator,” in *Conference on robot learning*. PMLR, 2017, pp. 1–16.

[14] M. Althoff, M. Koschi, and S. Manzinger, “Commonroad: Composable benchmarks for motion planning on roads,” in *2017 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2017, pp. 719–726.