2024 European Control Conference (ECC)
June 25-28, 2024. Stockholm, Sweden

Incremental Bayesian Learning for Fail-Operational Control in Autonomous Driving

Lei Zheng, Rui Yang, Zengqi Peng, Wei Yan, Michael Yu Wang, *Fellow, IEEE,* and Jun Ma

***Abstract*— Abrupt maneuvers by surrounding vehicles (SVs) can typically lead to safety concerns and affect the task efficiency of the ego vehicle (EV), especially with model uncertainties stemming from environmental disturbances. This paper presents a real-time fail-operational controller that ensures the asymptotic convergence of an uncertain EV to a safe state, while preserving task efficiency in dynamic environments. An incremental Bayesian learning approach is developed to facilitate online learning and inference of changing environmental disturbances. Leveraging disturbance quantification and constraint transformation, we develop a stochastic fail-operational barrier based on the control barrier function (CBF). With this development, the uncertain EV is able to converge asymptotically from an unsafe state to a defined safe state with probabilistic stability. Subsequently, the stochastic fail-operational barrier is integrated into an efficient fail-operational controller based on quadratic programming (QP). This controller is tailored for the EV operating under control constraints in the presence of environmental disturbances, with both safety and efficiency objectives taken into consideration. We validate the proposed framework in connected cruise control (CCC) tasks, where SVs perform aggressive driving maneuvers. The simulation results demonstrate that our method empowers the EV to swiftly return to a safe state while upholding task efficiency in real time, even under time-varying environmental disturbances.**

I. Introduction

With the rapid advancement of autonomous driving technology, ensuring the safety and reliability of autonomous vehicles (AVs) has become a paramount concern [1], [2]. One key underlying factor to this concern is the existence of model uncertainties resulting from unexpected environmental disturbances in high-speed driving scenarios [3], [4], such as changing road grade and aerodynamic drag. These factors necessitate high-speed AVs to continually adapt to inevitable disturbances to achieve safe and efficient operations. Additionally, the unpredictable maneuvers of surrounding vehicles (SVs), such as sudden deceleration, are challenging to anticipate. These unexpected maneuvers significantly influence the motion of the ego vehicle (EV), compromising driving efficiency and potentially leading to safety concerns [5]. This requires the EV to not only navigate safely under normal conditions but also promptly and effectively respond to these disturbances, such that continuous operation can be ensured. To achieve this target, the EV must react swiftly to sudden maneuvers of SVs and adapt to time-varying environmental disturbances in real time. This necessitates the development of an efficient fail-operational controller that operates at over $50\,\mathrm{Hz}$ to ensure that the EV reverts to a predefined safe state in the event of a fault (e.g., a safety violation) while maintaining its normal operational ability [6].

To effectively respond to hazardous situations, several works have focused on trajectory repairing for the EV [7]–[9]. While these works strive to replan infeasible trajectory segments to enhance safety, they lack formal safety assurance analysis. Furthermore, the repair frequency is slow, which is typically below $50\,\mathrm{Hz}$. This limitation hinders the EV's capacity to react swiftly to abrupt maneuvers executed by SVs in high-speed scenarios. To address these issues, researchers have employed reachability analysis to ensure the safety of the EV [10], [11]. For instance, a low-level safety-preserving controller running at $50\,\mathrm{Hz}$ has been developed to minimally intervene in unsafe actions based on the Hamilton-Jacobi reachability theory [11]. Additionally, control barrier functions (CBFs) have been adopted to ensure formal safety for safety-critical autonomous driving systems [12]–[14]. These methods involve the computation of a forward invariance safe set, serving as a hard constraint to realize safe interactions between the EV system and dynamic SVs. Although these works can provide formal safety assurances for deterministic systems, they may encounter challenges in ensuring the safety of the EV in the presence of model uncertainties resulting from environmental disturbances.

To cater to environmental disturbances, robust CBF has been developed [15]–[17]. In particular, to address the challenges posed by road and wind disturbances in high-speed autonomous driving scenarios, a disturbance observer-based safety-critical controller has been proposed for connected cruise control (CCC) tasks [16]. However, determining an appropriate robust bound remains a challenge due to the need to strike a balance between robustness and feasibility [17]. On the other hand, researchers have explored Bayesian learning approaches to quantify environmental disturbances. These estimated disturbances have been leveraged to develop stochastic CBFs [18]–[20], which provide formal safety

This work was supported in part by the National Natural Science Foundation of China under Grant 62303390; and in part by the Project of Hetao Shenzhen-Hong Kong Science and Technology Innovation Cooperation Zone under Grant HZQB-KCZYB-2020083. *(Corresponding Author: Jun Ma.)*

Lei Zheng, Rui Yang, Zengqi Peng, and Wei Yan are with the Robotics and Autonomous Systems Thrust, The Hong Kong University of Science and Technology (Guangzhou), Guangzhou, China (email: lzheng135@connect.ust.hk; ryang253@connect.hkust-gz.edu.cn; zpeng940@connect.ust.hk; wyan993@connect.hkust-gz.edu.cn).

Michael Yu Wang is with the School of Engineering, Great Bay University, Dongguan, China (email: mywang@gbu.edu.cn).

Jun Ma is with the Robotics and Autonomous Systems Thrust, The Hong Kong University of Science and Technology (Guangzhou), Guangzhou, China, also with the Division of Emerging Interdisciplinary Areas, The Hong Kong University of Science and Technology, Hong Kong SAR, China, and also with the HKUST Shenzhen-Hong Kong Collaborative Innovation Research Institute, Futian, Shenzhen, China (e-mail: jun.ma@ust.hk).

analysis for uncertain systems. For instance, an adaptive CBF has been introduced to enable safety-critical high-speed Mars rover missions, incorporating tractable Bayesian model learning [19]. Nonetheless, the learning process necessitates offline training due to its high computational complexity. To facilitate learning efficiency, an event-triggered mechanism is developed to update the Gaussian Process (GP) in model learning for safety-critical uncertain systems [20]. Despite these advancements, none of these works addresses safety recovery for the EV under environmental disturbances. It is worthwhile to mention that the capability of safety recovery becomes pivotal in autonomous driving scenarios when sudden maneuvers by SVs propel the EV into an unsafe state in the presence of uncertain environmental disturbances.

In this paper, we propose a real-time fail-operational controller for the EV in the presence of time-varying environmental disturbances. This controller is designed to guide autonomous vehicles back to a predefined safe state asymptotically, while upholding task efficiency. First, we devise an incremental learning strategy to reduce the online learning complexity of GPs from $O(n^3)$ to $O(n^2)$, thereby enabling the EV to adapt online to changing environmental disturbances effectively. Subsequently, a stochastic fail-operational barrier is developed by utilizing CBF in conjunction with the estimated environmental disturbances obtained through the incremental learning process. Rigorous theoretical analysis of probabilistic asymptotic stability is provided with the aim of converging the unsafe EV back to a defined safe set. Finally, we validate the effectiveness of the proposed fail-operational controller in a CCC task under time-varying environmental disturbances, demonstrating effective online learning and safety recovery for the EV.

The remainder of the paper is organized as follows: Section II presents the preliminaries and problem statement. In Section III, we detail the proposed methodology. Section IV demonstrates the numerical simulation of the proposed algorithm on an uncertain CCC system. Finally, Section V summarizes the key findings and insights of this study.

II. Preliminaries and problem statement

In this study, we consider the class of uncertain discrete-time nonlinear systems for the EV described by

$$x_{k+1} = F(x_k, u_k) = f(x_k) + \psi(x_k)u_k + w(x_k), \quad (1)$$

where $x_k \in \mathcal{X} \subset \mathbb{R}^n$, $u_k \in \mathcal{U} \subset \mathbb{R}^m$ and $w \in \mathcal{W} \subset \mathbb{R}^n$ denote the state, control, and uncertain disturbance vectors, respectively; $k \in \mathbb{Z}_+ = \{0, 1, \cdots\}$. The system matrix $f : \mathcal{X} \to \mathbb{R}^n$ and input matrix $\psi : \mathcal{U} \to \mathbb{R}^{n\times m}$ are local Lipschitz continuous. We make the following assumptions to tackle the uncertain disturbances in (1).

Assumption 1. The uncertain disturbance vector w has a bounded norm in the associated Reproducing Kernel Hilbert Space [21], corresponding to a differentiable kernel k.

Assumption 2. The following collection of state-disturbance trajectories is available:

$$\mathcal{D}_N := \left\{ \left(x^{(i)},\ \tilde{w}^{(i)} \right) \right\}_{i=1}^{N},\ \tilde{w}^{(i)} = w(x^{(i)}) + \upsilon_i, \quad (2)$$

where $N \in \mathbb{Z}_+$ denotes the number of samples; $\tilde{w}^{(i)} = [\tilde{w}_1^{(i)}, \tilde{w}_2^{(i)}, \cdots, \tilde{w}_n^{(i)}]^T$ denotes the i-th measured disturbance vector $w(x^{(i)}) = [w_1(x^{(i)}), w_2(x^{(i)}), \cdots, w_n(x^{(i)})]^T$ with independent and identically distributed white noise $\upsilon_i \sim \mathcal{N}\left(0, \sigma_{\text{noise}}^2 I_n\right)$.

Remark 1. Assumption 1 implies that the uncertain disturbance vector w is regular to the kernel and has a certain level of smoothness. This assumption further indicates the matrix F is local Lipschitz continuous on $\mathcal{X}$, ensuring the solution of (1) is unique and exits.

Consider the system (1), we further define the unsafe set, safe set, safe boundary, and interior safe set by a C^1 function $h : \mathbb{R}^n \to \mathbb{R}$ as follows:

$$Out(\mathcal{S}) = \{x \in \mathcal{X} \mid h(x) < 0\}, \quad (3a)$$
$$\mathcal{S} = \{x \in \mathcal{X} \mid h(x) \geq 0\}, \quad (3b)$$
$$\partial\mathcal{S} = \{x \in \mathcal{X} \mid h(x) = 0\}, \quad (3c)$$
$$Int(\mathcal{S}) = \{x \in \mathcal{X} \mid h(x) > 0\}. \quad (3d)$$

Definition 1. The continuous function $\gamma : (-c, d) \to (-c, d)$ is called an extended class $\mathcal{K}$ function for some $c, d \in \mathbb{R}^+$, if it is strictly increasing and satisfies the following conditions:

$$\gamma(h(x)) = \alpha h(x), \alpha \in (0, 1), \forall h(x) \neq 0, \quad (4a)$$
$$\gamma(0) = 0. \quad (4b)$$

Definition 2. ([22], [23]) The C^1 function h is called a discrete-time control barrier function (CBF) for the set $\mathcal{S}$ defined in (3a)-(3d), if there exists extend $\mathcal{K}$ functions γ with $\mathcal{S} \subset \mathcal{X}$, such that

$$\Delta h(x_k) + \gamma(h(x_{k-1})) > 0, \quad (5)$$

where $\Delta h(x_k) := h(x_k) - h(x_{k-1})$.

The goal of this work is to design a fail-operational controller for the uncertain nonlinear EV system (1) to accomplish specified tasks with the desired functionality, while satisfying the following two key objectives:

1) *Online adaptivity*: The EV system (1) can continuously adapt to time-varying environmental disturbances using newly collected interaction data in real time.
2) *Fail-operational control*: The EV system (1) can asymptotically converge to the safe set $\mathcal{S}$ from an unsafe state $Out(\mathcal{S})$, while upholding task efficiency.

III. Methodology

In this section, we first introduce an online incremental Bayesian learning approach to approximate the disturbances in the system (1). Then, we develop a stochastic fail-operational control barrier based on the quantified disturbances learned from interaction data with mathematical proof. Finally, We design an efficient fail-operational Quadratic Programming (QP) controller using stochastic optimization techniques.

A. Gaussian Process

As a typical Bayesian learning approach, the GP is a nonparametric method for learning complex functions and their uncertainty distributions [24]. In this study, we develop an incremental GP model that leverages Assumption 1 to learn the disturbance w using collected interaction data from the environment during operation.

Similar to [25], we assume disturbances are uncorrelated to train n independent GPs to approximate the nonlinear function $w : X \to \mathbb{R}^n$ as follows:

$$\hat{w}(x) = \begin{cases} \hat{w}_1(x) \sim \mathcal{N}(\mu_1(x),\ \sigma_1^2(x)) \\ \hat{w}_2(x) \sim \mathcal{N}(\mu_2(x),\ \sigma_2^2(x)) \\ \cdots \\ \hat{w}_n(x) \sim \mathcal{N}(\mu_n(x),\ \sigma_n^2(x)) \end{cases}. \tag{6}$$

Given N collected data pairs $\mathcal{D}_N := \left\{\left(x^{(i)},\ \tilde{w}^{(i)}\right)\right\}_{i=1}^{N}$, the mean and variance of the j-th component $\hat{w}_j(x_*)$ at the query state x_* can be inferred as:

$$\mu_j(x_*) = k_j^T (K_{\sigma,j} + \sigma_{\text{noise}}^2 I_N)^{-1} \tilde{w}_{N,j}, \tag{7a}$$

$$\sigma_j^2(x_*) = k_j(x_*, x_*) - k_{N,j}^T (K_{\sigma,j} + \sigma_{\text{noise}}^2 I_N)^{-1} k_{N,j}, \tag{7b}$$

where $\tilde{w}_{N,j} = [\tilde{w}_j^{(1)}, \tilde{w}_j^{(2)}, \cdots, \tilde{w}_j^{(N)}]^T \in \mathbb{R}^N$ denotes the observed vector. $K_{\sigma,j} \in \mathbb{R}^{N\times N}$ is the covariance matrix with entries $[K_{\sigma,j}]_{(i,q)} = k_j(x_i, x_q)$, $i, q \in \mathcal{I}_1^N = \{1, \cdots, N\}$, and $k_j(x_i, x_q)$ is the kernel function. $k_{N,j} = [k_j(x^{(1)}, x_*), k_j(x^{(2)}, x_*), \cdots, k_j(x^{(N)}, x_*)]^T \in \mathbb{R}^N$.

Lemma 1. ([26], [27]) Let $\varsigma \in (0,\ 1)$ and the measurement noise υ_j is uniformly bounded by σ_{noise}. Then a probability Pr holds

$$Pr\{\|\mu(x) - \delta(x)\| \le \|\beta\| \|\sigma(x)\|, \forall x \in \mathcal{X}\} \ge (1-\varsigma)^{2n}, \tag{8}$$

where $\beta = [\beta_1, \beta_2, \cdots, \beta_n]$, $\beta_j = (2\|\delta_j\|^2_{k_j} + 300\gamma_j ln^3(\frac{N+1}{\upsilon_j}))^{-2}$; γ_j is the maximum information gain obtained about the GP prior from N noisy samples as follows:

$$\gamma_j = \max_{x^{(1)},\ \ldots,\ x^{(N)} \in \mathcal{X}} \frac{1}{2} \log(\det(I_N - \frac{K_{\sigma,j}(x, x')}{\sigma_{\text{noise}}^2})), \tag{9}$$

where $x, x' \in \{x^{(1)},\ \ldots,\ x^{(N)}\}$.

B. Incremental Learning for Enhanced GPs

A significant challenge in the practical application of GPs is the computational burden associated with learning from large datasets. Incremental learning techniques can help to overcome this challenge through processing data streams in small increments, instead of processing the entire dataset at once [28], [29]. This technique enables the efficient updating of the GP model as new data becomes available, without retraining the entire model from scratch.

1) Active Learning: To effectively acquire labeled data points that offer the most valuable information for the incremental learning process, an active learning strategy is utilized. This strategy facilitates the selective and strategic acquisition of labeled data points, optimizing the learning progress and concurrently reducing the computational load associated with processing extensive datasets. In the context of incremental learning, we utilize uncertainty estimates provided by the GP model to select data points that are most informative for model updates. At each timestep, we calculate the uncertainty of each data point of the current kernel matrix using the covariance matrix provided by the GP model with the latest data point. Subsequently, we replace the least relevant data point, measured by the diagonal elements of the covariance matrix, with the latest data point for training purposes. This prioritization of labeling uncertain data points enables the incremental GP to focus on refining its predictions in regions of the input space where its confidence is low, thereby enhancing the estimation of disturbances in the current state.

We measure the relevance of data points using the squared Euclidean distance between each point and a new point of interest. To quantify this relevance, we employ a radial basis function (RBF) formulated as:

$$k(x_i, x_{\text{new}}) = \theta \exp\left(-\frac{1}{2l^2}\|x_i - x_{\text{new}}\|^2\right), \tag{10}$$

where x_{new} denotes the newly acquired data point, while x_i corresponds to the i-th data point in our kernel matrix. The parameter θ signifies the signal variance, playing a crucial role in regulating the scale of the kernel's output. l serves as the length scale parameter, dictating the rate where the similarity between data points diminishes with increasing distance.

2) Incremental Learning: With the informative data point selected by the active learning strategy , we leverage the Woodbury matrix identity to efficiently update the GP's kernel matrix and its inverse in an incremental way.

We denote the current kernel matrix and its inverse as $K_{\sigma,\text{cur}} \in \mathbb{R}^{N\times N}$ and $K_{\sigma,\text{cur}}^{-1} \in \mathbb{R}^{N\times N}$, respectively. We assume the dataset has reached its predefined size. At each time step, we add a newly collected interaction data point to the dataset and simultaneously remove the one with the lowest similarity based on (10) from the current kernel matrix.

The current kernel matrix $K_{\sigma,\text{cur}}$ can be represented in block matrix form as:

$$K_{\sigma,\text{cur}} = \begin{bmatrix} k_0 & k_{N-1}^T \\ k_{N-1} & \Omega \end{bmatrix}, \tag{11}$$

where $k_0 \in \mathbb{R}$ and $k_{N-1} \in \mathbb{R}^{N-1}$ represent the variance and covariance vector of the data point that exhibits the lowest similarity with the newly collected data point in the dataset, respectively; $\Omega \in \mathbb{R}^{(N-1)\times(N-1)}$ is the sub-matrix at the right bottom corner.

The inverse matrix of $K_{\sigma,\text{cur}}$ can be computed as:

$$K_{\sigma,\text{cur}}^{-1} = \begin{bmatrix} \rho_0 & \rho_{N-1}^T \\ \rho_{N-1} & S \end{bmatrix}, \tag{12}$$

where $\rho_0 \in \mathbb{R}$, $\rho_{N-1} \in \mathbb{R}^{N-1}$, and $S \in \mathbb{R}^{(N-1)\times(N-1)}$.

To derive the updated kernel matrix $K_{\sigma,\text{new}}$, the following procedure is implemented as outlined in [29]: Initially, we remove the least relevant data point chosen by the active

learning strategy from the current dataset. Next, we compute the variance $k_{0,\text{new}} \in \mathbb{R}$ and the covariance vector $k_{N-1,\text{new}} \in \mathbb{R}^{N-1}$ corresponding to the newly introduced data point. The resulting new kernel matrix $K_{\sigma,\text{new}}$ is obtained as:

$$K_{\text{new}} = \begin{bmatrix} \Omega & k_{N-1,\text{new}} \\ k_{N-1,\text{new}}^T & k_{0,\text{new}} + \sigma_{\text{noise}}^2 I \end{bmatrix}, \tag{13}$$

where $\sigma_{\text{noise}}^2 I$ is the noise covariance matrix.

The inverse matrix of K_{new} can be computed using the Woodbury matrix identity as follows:

$$K_{\text{new}}^{-1} = \begin{bmatrix} P + Pk_{N-1,\text{new}}(Pk_{N-1,\text{new}})^T Q & -Pk_{N-1,\text{new}}Q \\ -(Pk_{N-1,\text{new}})^T Q & Q \end{bmatrix}, \tag{14}$$

where $P = \Omega - \rho_{N-1} \cdot \rho_{N-1}^T \rho_0^{-1} \in \mathbb{R}^{(N-1)\times(N-1)}$ and $Q = (k_{0,\text{new}} + \sigma_{\text{noise}}^2 I - k_{N-1,\text{new}}^T Pk_{N-1,\text{new}})^{-1} \in \mathbb{R}$.

Note that the Woodbury matrix identity involves several matrix multiplications, resulting in a computational complexity of $O(N^2)$ for this increment learning, where N represents the size of the dataset. Therefore, this approach is computationally efficient compared to the traditional GP, which requires the inversion of the entire kernel matrix and has a computational complexity of $O(N^3)$.

To further improve the learning performance, we optimize the kernel hyperparameters of the RBF kernel k_j (7) using the log-marginal likelihood function of the following form:

$$\begin{aligned} \log p(\tilde{w}_{N,j}|X_N, \Theta_j) = &\frac{1}{2}\tilde{w}_{N,j}^T (K_N + \theta_{f,j}^2 I_N)^{-1} \tilde{w}_{N,j} \\ &+ \frac{1}{2}\log\left|K_N + \theta_{f,j}^2 I_N\right| + \frac{N}{2}\log(2\pi), \end{aligned} \tag{15}$$

where $\tilde{w}_{N,j} = [\tilde{w}_j^{(1)}, \tilde{w}_j^{(2)}, \cdots, \tilde{w}_j^{(N)}]^T$ denotes the observed disturbances vector; $X_N = [x^{(1)}, x^{(2)}, \cdots, x^{(N)}]^T$ denotes the corresponding state vector; $\Theta_j = [\theta_{f,j}, l_{f,j}]^T$ denotes the kernel hyperparameters of the following RBF function:

$$k_j(x^{(i)},\ x^{(j)}) = \theta_{f,j} \exp\left(-\frac{1}{l_{f,j}^2}||x^{(i)} - x^{(j)}||^2\right). \tag{16}$$

This optimization is performed online using a validation set as follows:

$$(\theta_{f,j}^*, l_{f,j}^*) = \underset{(\theta_{f,j}, l_{f,j}) \in \mathbb{R}\times\mathbb{R}}{\text{minimize}} \quad \log p(\tilde{w}_{N,j}|X_N, \theta_{f,j}, l_{f,j}), \tag{17}$$

$$\text{subject to} \quad \theta_{f,j}(0) = \theta_{f,0}, \tag{18}$$

$$l_{f,j}(0) = l_{f,0}, \tag{19}$$

$$\theta_{f,min} \le \theta_{f,j} \le \theta_{f,max}, \tag{20}$$

$$l_{f,min} \le l_{f,j} \le l_{f,max}, \tag{21}$$

where $\theta_{f,0}$ and $l_{f,0}$ represent the initial kernel hyperparameters; $\theta_{f,min}$ and $\theta_{f,max}$ represent the minimum and maximum value for the kernel hyperparameter θ_f, respectively; $l_{f,min}$ and $l_{f,max}$ represent the minimum and maximum value for the kernel hyperparameter l, respectively.

To solve this bound constrained optimization problem (17)-(21), we employ the L-BFGS-B optimization algorithm [30]. This iterative method approximates the inverse Hessian matrix of the objective function, allowing us to find the optimal set of hyperparameters while adhering to the specified bounds for each hyperparameter.

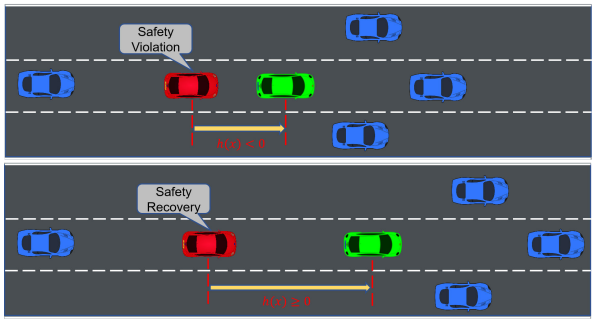


Fig. 1. The stochastic fail-operational barrier module enables the red EV to recover from an unsafe state (top subfigure) to a safe state (bottom subfigure).

C. Stochastic Fail-Operational Barrier

We aim to design a stochastic fail-operational barrier module that ensures the uncertain EV converges from the unsafe state $Out(\mathcal{S})$ to a safe state $\mathcal{S}$ and remains in the safe state after recovery, as depicted in Fig. 1.

Lemma 2. *Let $D_w = [\mu(x_{k-1}) - c\sigma(x_{k-1}), \mu(x_{k-1}) + c\sigma(x_{k-1})], c \in \mathbb{R}^+$ represents the high-confidence disturbances set approximated by (7) for the uncertain nonlinear system (1) under Assumptions 1-2. Then the unsafe state $x_0 \in Out(\mathcal{S})$ asymptotically converges to safe set $\mathcal{S}$ with probability at least $(1-\varsigma)^{2n}$ by the following constraint:*

$$\begin{aligned} h(f(x_{k-1})) + &h(\psi(x_{k-1})u_{k-1} + \epsilon(w(x_{k-1})) \\ &> h(x_{k-1}) - \gamma(h(x_{k-1})), \end{aligned} \tag{22}$$

where $\epsilon(w(x_{k-1})) = h(\mu(x_{k-1})) - c\|h(\sigma(x_{k-1}))\|$, and the barrier function h takes the form of an affine function.

Proof. From Lemma 1, we obtain

$$Pr\{w(x_{k-1}) \in D_w\} \ge (1-\varsigma)^{2n}. \tag{23}$$

Utilizing the properties of the affine barrier function h, we obtain:

$$Pr\{h(w(x_{k-1})) \ge \epsilon(w(x_{k-1}))\} \ge (1-\varsigma)^{2n}. \tag{24}$$

Consequently, the following result holds with a probability of at least $(1-\varsigma)^{2n}$:

$$\begin{aligned} &h(f(x_{k-1})) + h(\psi(x_{k-1})u_{k-1}) + h(w(x_{k-1})) \\ &\ge h(f(x_{k-1})) + h(\psi(x_{k-1}))u_{k-1} + \epsilon(w(x_{k-1})) \\ &> h(x_{k-1}) - \gamma(h(x_{k-1})). \end{aligned} \tag{25}$$

This yields:

$$Pr\{h(x_k) > h(x_{k-1}) - \gamma(h(x_{k-1})\} \ge (1-\varsigma)^{2n}. \tag{26}$$

With Definition 1, we deduce the following results with probability at least $(1-\varsigma)^{2n}$:

$$\begin{aligned} &h(x_k) - (h(x_{k-1}) - \gamma(h(x_{k-1})) \\ &= h(x_k) - (1-\alpha)h(x_{k-1}) > 0. \end{aligned} \tag{27}$$

Hence, $h(x_k) > (1-\alpha)h(x_{k-1})$, where $\alpha \in (0,1)$. It yields:

$$Pr\{h(x_k) \geq (1-\alpha)h(x_{k-1})\} \geq (1-\varsigma)^{2n}. \tag{28}$$

This result indicates that the state of the EV with $h(x_0) < 0$ will asymptotically converge to the safe set $\mathcal{S}$ at a rate of at least $(1-\alpha)^k$ over k steps of evolution. □

Remark 2. The constraint presented in (28) has significant implications for the behavior of the uncertain nonlinear system (1) when the system is inside the safe set $\mathcal{S}$, where $h(x_k) \geq 0$. This constraint ensures that, once the system enters the safe set, it remains within this region, guaranteeing the forward invariance of the safe set $\mathcal{S}$. This critical property has been discussed in detail in [23].

D. Real-Time Fail- Operational Controller

The fail-operational controller aims to achieve the desired task performance specified by fail-operational control criteria, as outlined in [6]. This requires the fail-operational controller to repair the undesired state while upholding task efficiency. Considering the input constraints of the uncertain nonlinear EV system (1), we introduce the following computational-efficiency fail-operational controller in a QP formulation:

$$\begin{aligned} u_k^* = \underset{u_k \in \mathbb{R}^m}{\operatorname{argmin}} \quad & \|u_k\|^2 + \lambda_\varsigma \zeta^2 + \lambda_\iota \iota^2, && (29)\\ \text{subject to} \quad & h(f(x_k)) + h(\psi(x_k))u_k + \epsilon(w(x_k)) \\ & > h(x_k) - \gamma(h(x_k)) - \zeta, && (30)\\ & \Delta V(x_k) + c_v V(x_k) < \iota, && (31)\\ & u_{\min} \leq u_k \leq u_{\max}, && (32) \end{aligned}$$

where $u_{\min}$ and $u_{\max}$ denote the minimum and maximum control input value, respectively; $\zeta, \iota \in \mathbb{R}^+$ are non-negative slack variables used to ensure the feasibility of the constrained optimization problem (29)-(32); λ_ζ and $\lambda_\iota \in \mathbb{R}^+$ are corresponding weights; $\Delta V(x_k) = V(x_{k+1}) - V(x_k)$, where V is a discrete-time exponentially stabilizing control Lyapunov function (ES-CLF) [31] utilized to encode the desired state for the EV, and the constraint (31) is specifically crafted to stabilize the uncertain nonlinear EV system (1) toward this desired state, which can be further transformed into a deterministic constraint with the estimated disturbances set D_w based on [32].

Remark 3. The parameters λ_ζ is assigned a large penalization weight to enforce the constraint ζ to be a negligible value, thereby minimizing its influence on the stochastic fail-operational barrier constraint (22). Furthermore, λ_ζ is greater than λ_ι to prioritize safety over task performance. According to Lemma 2, when constraint (22) is satisfied, the fail-operational control obtained by solving the QP problem (29)-(32) can effectively navigate the EV from an unsafe state $x \in Out(\mathcal{S})$ back to the safe set $\mathcal{S}$ with a high probability of at least $(1-\varsigma)^{2n}$.

TABLE I
PARAMETERS OF VEHICLE MODEL

k_v	$0.25\,\mathrm{N}\cdot\mathrm{s}^2/\mathrm{m}^2$	α_i	30
β_i	2000	l_i	2.91 m
M	1650 kg	g	$9.81\,\mathrm{m/s}^2$
$\phi_{\min}$	-10 deg	$\phi_{\max}$	10 deg
$v_{\max}$	40 m/s		

IV. ILLUSTRATIVE EXAMPLE

In this section, we evaluate the effectiveness of the proposed real-time fail-operational controller in CCC driving tasks. The CCC system consists of one EV and four human-driven vehicles (HVs) exhibiting sudden acceleration and deceleration behaviors in the presence of time-varying environmental disturbances.

A. Vehicle Model

The uncertain nonlinear EV system dynamics are formulated as follows:

$$\dot{x} = \begin{bmatrix} \dot{p} \\ \dot{v} \end{bmatrix} = \begin{bmatrix} v_E \\ -\frac{F_f + F_r}{M} - a(\phi) \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{M} \end{bmatrix} u_E, \tag{33}$$

where M denotes the mass of the EV; $u_E \in [-0.3gM, 0.3gM]$ denotes the control input, g is the gravitational acceleration; p and v represent the position and velocity of the EV, respectively. F_f, F_r, and $a(\phi)$ correspond to the aerodynamic drag, rolling resistance, and road grade, defined as follows:

$$F_f = k_v v^2, \quad F_r = k_f(t) gM\cos(\phi), \quad a(\phi) = g\sin(\phi), \tag{34}$$

where k_v and k_f represent the coefficients for aerodynamic drag and road resistance, respectively; ϕ represents the road grade. The k_f is assumed to be a constant value of 0.06, while k_v and ϕ are set to zero to introduce uncertain disturbances for the EV. We discrete the systems (33) using the Euler method with a discrete interval of $T_s = 0.02\,\mathrm{s}$.

We define the state of the i-th HV as $O^i = [s^i, v^i]^T$, where s^i and v^i represent the position and velocity of the i-th HV, respectively. The desired control input of the i-th HV in the CCC system are adopted from [33]:

$$u_k^i = \alpha_i(K_i(d_k^i) - v_k^i) + \beta_i(v_k^{i+1} - v_k^i), \tag{35}$$

where $d_k^i = s_k^{i+1} - s_k^i - l_i$ denotes the headway of the i-th HV at time step k; l_i denotes the length of the i-th HV; α_i and β_i denote the control gain coefficients of the i-th HV. The range function K_i is used to describe the target velocity for the i-th HV as follows:

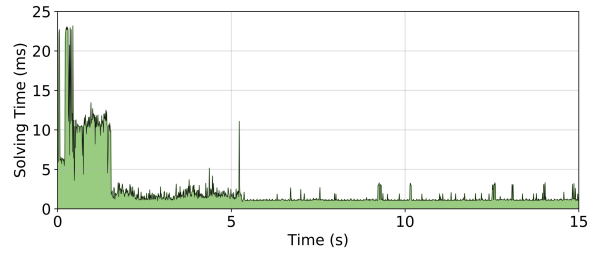
$$K_i(d_k^i) = \begin{cases} 0 & \text{if } d_k^i \leq d_{\min}^i, \\ k_i(d_k^i - d_{\min}^i) & \text{if } d_{\min}^i < d_k^i < d_{\max}^i, \\ v_{\max} & \text{if } d_k^i \geq d_{\max}^i, \end{cases} \tag{36}$$

where $v_{\max}$ denotes the maximum velocity and $k_i = \frac{v_{\max}}{d_{\max}^i - d_{\min}^i}$. The small headway $d_{\min}^i$ and large headway $d_{\max}^i$ indicate where the i-th HV intends to stop and travel, respectively. The vehicle parameters are listed in Table I.

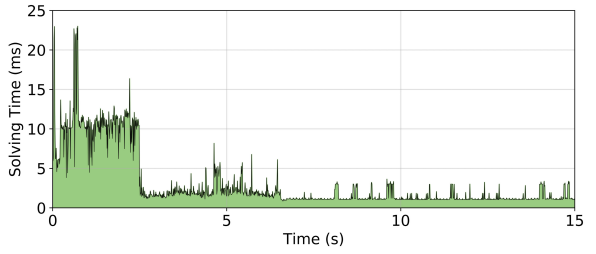
TABLE II

AVERAGE COMPUTATION TIME FOR DIFFERENT INITIAL STATES IN THE CCC TASK UNDER TIME-VARYING ENVIRONMENTAL DISTURBANCES.

Initial State x_0	QP solving	Learning	Inference
$[25\,\text{m}, 18\,\text{m/s}]^T$	2.349 ms	4.696 ms	0.032 ms
$[110\,\text{m}, 18\,\text{m/s}]^T$	3.035 ms	4.241 ms	0.034 ms



(a)



(b)

Fig. 2. The evolution of solving time of the optimization problem (29)-(32) with two unsafe initial states. (a) Initial state $x_0 = [25\,\text{m}, 18\,\text{m/s}]^T$, (b) Initial state $x_0 = [110\,\text{m}, 18\,\text{m/s}]^T$.

B. Simulation Setup

Our simulation experiments were conducted on an Ubuntu 20.04 LTS system with an AMD Ryzen 7 5800H CPU with eight cores and sixteen threads. It operates at a base clock speed of 2.28 GHz, with a maximum boost frequency of 3.20 GHz and a minimum frequency of 1.20 GHz. The system is equipped with 16 GB of RAM. We utilize the CVXOPT as the solver for the QP problem (29)-(32) based on Python 3.7.

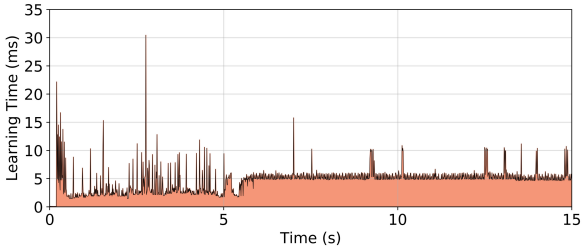
The initial states of the HVs are set as $O_0^1 = [240\,\text{m}, 18\,\text{m/s}]^T$, $O_0^2 = [180\,\text{m}, 18\,\text{m/s}]^T$, $O_0^3 = [120\,\text{m}, 18\,\text{m/s}]^T$, $O_0^4 = [0\,\text{m}, 18\,\text{m/s}]^T$. The EV between the third and fourth HV aims to cruise at a target speed $v_g = 20\,\text{m/s}$ in a one-direction road while keeping a desired following distance $[d_1, d_2]$ with its front HV. To achieve this goal, we design four independent GPs to model the state disturbances for the uncertain EV and its front HV. The following CBF and ES-CLF functions are designed:

$$h_1(x_k) = s_k^3 - p_k - d_1, \tag{37a}$$

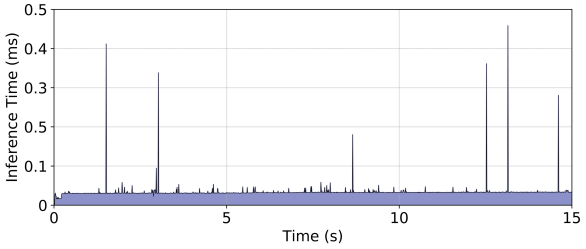
$$h_2(x_k) = -s_k^3 + p_k + d_2, \tag{37b}$$

$$V(x_k) = \|v - v_d\|^2. \tag{38}$$

The following parameters are used : $N = 20$, $\sigma_{\text{noise}} = 10^{-6}$, $\theta_{f,0} = 1$, $\theta_{f,min} = 10^{-3}$, $\theta_{f,max} = 10^3$, $l_{f,0} = 1$, $l_{f,min} = 10^{-2}$, $l_{f,max} = 10^2$, $c = 3$, $\alpha = 0.05$, $c_v = 0.8$, $\lambda_\zeta = 10^{30}$, $\lambda_\iota = 10^{10}$, $d_1 = d_{\text{min}}^i = 25\,\text{m}$, $d_2 = d_{\text{max}}^i = 100\,\text{m}$ and

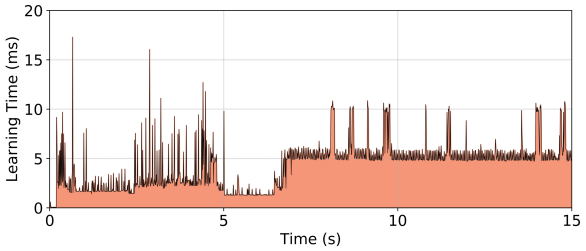


(a) Learning Time

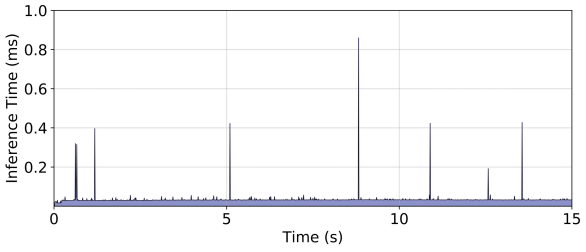


(b) Inference Time

Fig. 3. The evolution of incremental learning and inference time with the initial state $x_0 = [110\,\text{m}, 18\,\text{m/s}]^T$.



(a) Learning Time



(b) Inference Time

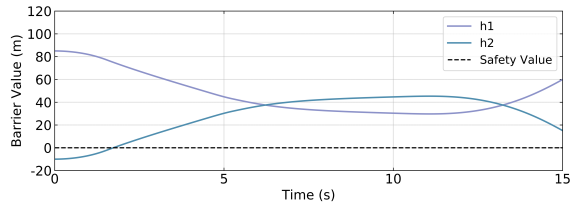
Fig. 4. The evolution of incremental learning and inference time with the initial state $x_0 = [25\,\text{m}, 18\,\text{m/s}]^T$.

$v_d = 20\,\text{m/s}$. The simulation duration and control frequency are set at 15 s and 50 Hz, respectively.

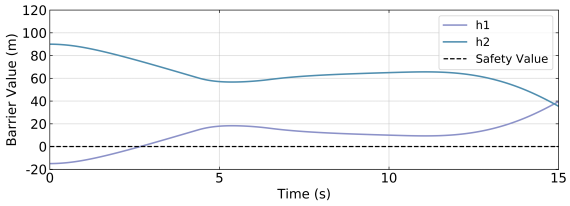
C. Results

The initial state x_0 of the EV is set as $[25, \text{m}, 18, \text{m/s}]^T$ and $[110, \text{m}, 18, \text{m/s}]^T$, leading to two unsafe initial state configurations with $h_2 < 0$ and $h_1 < 0$ for the EV, respectively. We assess the real-time and task performance in achieving a safe following distance and desired cruise speeds in the presence of time-varying environmental disturbances.

1) Real-Time Performance: Table II and Fig. 2 depict the average and evolution of the computation time for the fail-operational controller (29)-(32), with different initial states. The average solving times are 2.349 ms and 3.035 ms for



(a)



(b)

Fig. 5. The evolution of the CBF value for the EV with two different unsafe initial states. (a) $x_0 = [25\,\text{m}, 18\,\text{m/s}]^T$, (b) $x_0 = [110\,\text{m}, 18\,\text{m/s}]^T$. The negative CBF can quickly converge to positive values and remain positive throughout the CCC task in the presence of environmental disturbances.

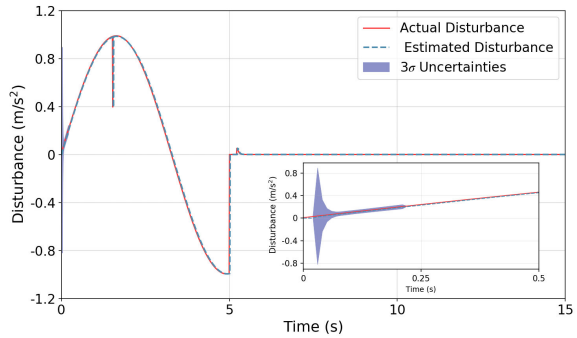


Fig. 6. The estimated time-varying disturbance of the EV in the acceleration aspect, with an initial state of $x_0 = [25\,\text{m}\ 18\,\text{m/s}]$. The abrupt disturbance fluctuations result from a sudden change in the road resistance coefficient. The embedding figure illustrates the evolution of model disturbance from 0 s to 0.5 s.

initial state $x_0 = [25\,\text{m}, 18\,\text{m/s}]^T$ and $x_0 = [110\,\text{m}, 18\,\text{m/s}]^T$, respectively. Regarding the incremental learning process and inference shown in Fig. 3 and Fig. 4. It is evident that both learning and inference time remain consistently low, with averages of less than 5 ms and 0.4 ms, respectively. Notably, these durations collectively sum to less than 20 ms on average, thus ensuring the feasibility of real-time optimization, learning, and inference. Moreover, one can notice that the optimization time is relatively large during the intervals from 0 s to 1.74 s and 2.54 s, as shown in Fig. 2(a) and Fig. 2(b), respectively. During these specific time intervals, the fail-operational controller diligently endeavors to restore the EV to a safe state within its designated safe set, characterized by the conditions $h_1 > 0$ and $h_2 > 0$, as depicted in Fig. 5.

2) Task Performance: Consider the EV's initial state denoted as $x_0 = [25\,\text{m}, 18\,\text{m/s}]^T$ as a case in point. The incremental learning performance in modeling the disturbances is illustrated in Fig. 6. One can notice that the estimated high-confidence uncertainties (at the 3σ level) exhibit an initial decrease, maintaining a consistently low value. This indicates

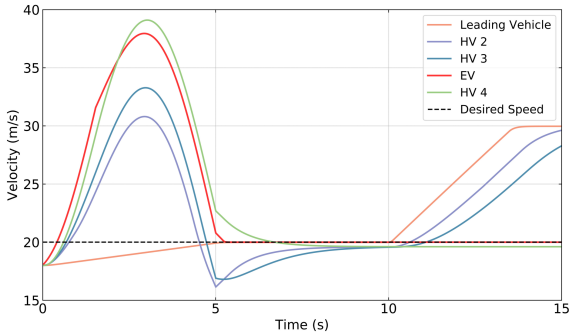


Fig. 7. The evolution of velocity for each vehicle in the CCC system led by the first HV. The similarities in the velocity profiles indicate how other vehicles attempt to adjust their speed to follow their front vehicle.

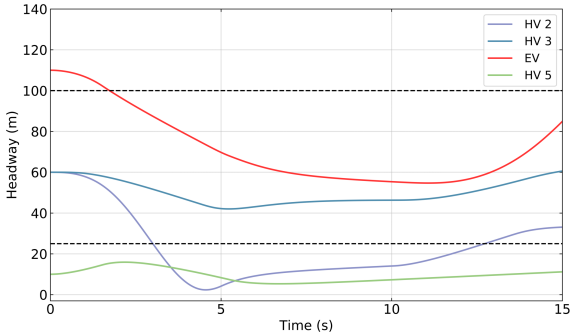


Fig. 8. The headway evolution for other vehicles in the CCC system led by the first HV, where the two dashed black lines denote the target headway.

that the proposed incremental learning method is capable of effectively adapting to uncertain disturbances, leveraging real-time interaction data.

Figure 7 illustrates the temporal evolution of driving speeds for each vehicle. The EV accelerates to follow its front vehicle (HV 3) in the very beginning to drive its unsafe state back to the safe state, as evidenced by the CBF value h_2 and the EV's headway, which are depicted in Fig. 5(a) and Fig. 8, respectively. In the presence of road and aerodynamic drag disturbances, as shown in Fig. 6, the distance between HV 2 and its front leading vehicle (HV 1) falls below the desired headway threshold of 25 m at 3.5 s. Consequently, the HV 2 promptly reduces its speed to maintain a safe following distance, causing an urgent deceleration of HV 3 from 3.5 s to 5 s. As expected, the EV also reduces its speed to ensure a safe following distance. Notably, once it returns to a safe state, the EV consistently maintains the desired headway distance, whereas HV 2 and HV 5 struggle to maintain the desired following distance, as shown in Fig. 8. These observations underscore the capability of the EV to return to a safe state even in the presence of road and air drag disturbances and rapid acceleration and deceleration behaviors exhibited by HVs.

In terms of task accuracy, the EV can quickly achieve a desired cruise speed $v_d = 20\,\text{m/s}$ around 5 s, while keeping a desired following distance with its front uncertain HV 3. This accomplishment underscores the effectiveness of the proposed fail-operational controller, as it ensures that the primary driving task is not significantly compromised. This

finding further supports the high task performance for the EV, aligning with our goal of achieving fail-operational control while upholding travel efficiency.

V. Conclusions

This paper proposes a real-time fail-operational controller for autonomous driving systems, which can adapt to changing environmental disturbances while adhering to state and input constraints. This controller integrates incremental Bayesian learning and control theory, enabling the EV to achieve its desired performance while remaining adaptable to environmental disturbances. Our simulation results on a CCC task have substantiated the efficacy of our fail-operational controller, showcasing its ability to safely guide an unsafe EV to a safe state while sustaining the desired performance. This achievement was maintained despite the high-velocity HV exhibiting urgent acceleration and deceleration behaviors, along with road and aerodynamic drag disturbances.

References

[1] L. Chen, Y. Li, C. Huang, B. Li, Y. Xing, D. Tian, L. Li, Z. Hu, X. Na, Z. Li *et al.*, "Milestones in autonomous driving and intelligent vehicles: Survey of surveys," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 2, pp. 1046–1056, 2022.

[2] J. Ma, Z. Cheng, X. Zhang, M. Tomizuka, and T. H. Lee, "Alternating direction method of multipliers for constrained iterative LQR in autonomous driving," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 23 031–23 042, 2022.

[3] A. Brandt, B. Jacobson, and S. Sebben, "High speed driving stability of road vehicles under crosswinds: an aerodynamic and vehicle dynamic parametric sensitivity analysis," *Vehicle System Dynamics*, vol. 60, no. 7, pp. 2334–2357, 2022.

[4] J. Knaup, K. Okamoto, and P. Tsiotras, "Safe high-performance autonomous off-road driving using covariance steering stochastic model predictive control," *IEEE Transactions on Control Systems Technology*, 2023.

[5] L. Zheng, R. Yang, Z. Peng, H. Liu, M. Y. Wang, and J. Ma, "Real-time parallel trajectory optimization with spatiotemporal safety constraints for autonomous driving in congested traffic," in *IEEE International Conference on Intelligent Transportation Systems*, 2023, pp. 1186–1193.

[6] T. Stolte, S. Ackermann, R. Graubohm, I. Jatzkowski, B. Klamann, H. Winner, and M. Maurer, "Taxonomy to unify fault tolerance regimes for automotive systems: Defining fail-operational, fail-degraded, and fail-safe," *IEEE Transactions on Intelligent Vehicles*, vol. 7, no. 2, pp. 251–262, 2021.

[7] Y. Lin, S. Maierhofer, and M. Althoff, "Sampling-based trajectory repairing for autonomous vehicles," in *IEEE International Intelligent Transportation Systems Conference*, 2021, pp. 572–579.

[8] C. Rösmann, W. Feiten, T. Wösch, F. Hoffmann, and T. Bertram, "Trajectory modification considering dynamic constraints of autonomous robots," in *German Conference on Robotics*, 2012, pp. 1–6.

[9] J. Ziegler, P. Bender, T. Dang, and C. Stiller, "Trajectory planning for bertha—a local, continuous method," in *IEEE Intelligent Vehicles Symposium Proceedings*, 2014, pp. 450–457.

[10] C. Pek and M. Althoff, "Fail-safe motion planning for online verification of autonomous vehicles using convex optimization," *IEEE Transactions on Robotics*, vol. 37, no. 3, pp. 798–814, 2020.

[11] X. Wang, K. Leung, and M. Pavone, "Infusing reachability-based safety into planning and control for multi-agent interactions," in *IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2020, pp. 6252–6259.

[12] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *European Control Conference*, 2019, pp. 3420–3431.

[13] S. He, J. Zeng, and K. Sreenath, "Autonomous racing with multiple vehicles using a parallelized optimization with safety guarantee using control barrier functions," in *International Conference on Robotics and Automation*, 2022, pp. 3444–3451.

[14] L. Zheng, R. Yang, M. Y. Wang, and J. Ma, "Barrier-enhanced homotopic parallel trajectory optimization for safety-critical autonomous driving," *arXiv preprint arXiv:2402.10441*, 2024.

[15] A. Robey, L. Lindemann, S. Tu, and N. Matni, "Learning robust hybrid control barrier functions for uncertain systems," *IFAC-PapersOnLine*, vol. 54, no. 5, pp. 1–6, 2021.

[16] A. Alan, T. G. Molnar, E. Daş, A. D. Ames, and G. Orosz, "Disturbance observers for robust safety-critical control with control barrier functions," *IEEE Control Systems Letters*, vol. 7, pp. 1123–1128, 2022.

[17] Q. Nguyen and K. Sreenath, "Robust safety-critical control for dynamic robotics," *IEEE Transactions on Automatic Control*, vol. 67, no. 3, pp. 1073–1088, 2021.

[18] L. Zheng, R. Yang, J. Pan, H. Cheng, and H. Hu, "Learning-based safety-stability-driven control for safety-critical systems under model uncertainties," in *International Conference on Wireless Communications and Signal Processing*, 2020, pp. 1112–1118.

[19] D. D. Fan, J. Nguyen, R. Thakker, N. Alatur, A.-a. Agha-mohammadi, and E. A. Theodorou, "Bayesian learning-based adaptive control for safety critical systems," in *IEEE International Conference on Robotics and Automation*, 2020, pp. 4093–4099.

[20] Z. Wu, R. Yang, L. Zheng, and H. Cheng, "Safe learning-based feedback linearization tracking control for nonlinear system with event-triggered model update," *IEEE Robotics and Automation Letters*, vol. 7, no. 2, pp. 3286–3293, 2022.

[21] B. Scholkopf and A. J. Smola, Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond. Cambridge, MA, USA: MIT press, 2018.

[22] M. Ahmadi, A. Singletary, J. W. Burdick, and A. D. Ames, "Safe policy synthesis in multi-agent pomdps via discrete-time barrier functions," in *IEEE Conference on Decision and Control*, 2019, pp. 4797–4803.

[23] J. Zeng, Z. Li, and K. Sreenath, "Enhancing feasibility and safety of nonlinear model predictive control with discrete-time control barrier functions," in *IEEE Conference on Decision and Control*, 2021, pp. 6137–6144.

[24] M. P. Deisenroth, D. Fox, and C. E. Rasmussen, "Gaussian processes for data-efficient learning in robotics and control," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 37, no. 2, pp. 408–423, 2013.

[25] C. J. Ostafew, A. P. Schoellig, and T. D. Barfoot, "Robust constrained learning-based nmpc enabling reliable mobile robot path tracking," *The International Journal of Robotics Research*, vol. 35, no. 13, pp. 1547–1563, 2016.

[26] N. Srinivas, A. Krause, S. M. Kakade, and M. W. Seeger, "Information-theoretic regret bounds for gaussian process optimization in the bandit setting," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3250–3265, 2012.

[27] J. Umlauft, L. Pöhler, and S. Hirche, "An uncertainty-based control lyapunov approach for control-affine systems modeled by gaussian process," *IEEE Control Systems Letters*, vol. 2, no. 3, pp. 483–488, 2018.

[28] Y. Wu, Y. Chen, L. Wang, Y. Ye, Z. Liu, Y. Guo, and Y. Fu, "Large scale incremental learning," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2019, pp. 374–382.

[29] L. Zheng, R. Yang, Z. Wu, J. Pan, and H. Cheng, "Safe learning-based gradient-free model predictive control based on cross-entropy method," *Engineering Applications of Artificial Intelligence*, vol. 110, p. 104731, 2022.

[30] J. L. Morales and J. Nocedal, "Algorithm 778: L-BFGS-B: Fortran subroutines for large-scale bound-constrained optimization"," *ACM Transactions on Mathematical Software*, vol. 23, no. 4, pp. 550–560, 1997.

[31] A. Agrawal and K. Sreenath, "Discrete control barrier functions for safety-critical control of discrete systems with application to bipedal robot navigation." in *Robotics: Science and Systems*, vol. 13, 2017, pp. 1–10.

[32] F. Castaneda, J. J. Choi, B. Zhang, C. J. Tomlin, and K. Sreenath, "Gaussian process-based min-norm stabilizing controller for control-affine systems with uncertain input effects and dynamics," in *American Control Conference*, 2021, pp. 3683–3690.

[33] C. R. He, I. G. Jin, and G. Orosz, "Data-based fuel-economy optimization of connected automated trucks in traffic," in *American Control Conference*, 2018, pp. 5576–5581.