

Control Barrier Functions and Input-to-State Safety with Application to Automated Vehicles

Anil Alan¹, Andrew J. Taylor², Chaozhe R. He^{1,3}, Aaron D. Ames², and Gábor Orosz^{1,4}

Abstract—Balancing safety and performance is one of the predominant challenges in modern control system design. Moreover, it is crucial to robustly ensure safety without inducing unnecessary conservativeness that degrades performance. In this work we present a constructive approach for safety-critical control synthesis via *Control Barrier Functions* (CBF). By filtering a hand-designed controller via a CBF, we are able to attain performant behavior while providing rigorous guarantees of safety. In the face of disturbances, robust safety and performance are simultaneously achieved through the notion of *Input-to-State Safety* (ISSf). We take a tutorial approach by developing the CBF-design methodology in parallel with an inverted pendulum example, making the challenges and sensitivities in the design process concrete. To establish the capability of the proposed approach, we consider the practical setting of safety-critical design via CBFs for a *connected automated vehicle* (CAV) in the form of a class-8 truck without a trailer. Through experimentation we see the impact of unmodeled disturbances in the truck’s actuation system on the safety guarantees provided by CBFs. We characterize these disturbances and using ISSf, produce a robust controller that achieves safety without conceding performance. We evaluate our design both in simulation, and for the first time on an automotive system, experimentally.

Index Terms—Robust safety-critical control, control barrier functions, input-to-state safety, connected automated vehicles.

I. INTRODUCTION

Safety is an ever more pressing requirement for modern control systems as they are deployed into increasingly complex real-world environments. Simultaneously, meeting performance requirements is a major driving factor in control system design. As these two objectives may naturally oppose each other, it is necessary to consider an *active* approach for enforcing safety that impacts performance only when it is critical for the safety of the system [1], [2]. *Control Barrier Functions* (CBFs) have been demonstrated to be a powerful tool for constructively synthesizing controllers that yield strong performance and intervene only when safety is at risk of being compromised [3]–[5]. The utility of CBFs has been confirmed by their experimental application on real-world control systems, including mobile robots [1], [6], robotic

This research is supported in part by the National Science Foundation, CPS Award #1932091.

¹A. Alan, C. R. He, and G. Orosz are with the Department of Mechanical Engineering, University of Michigan, Ann Arbor, MI 48109, USA {anilalan, hchaozhe, orosz}@umich.edu

²A. J. Taylor and A. D. Ames are with the Department of Computing & Mathematical Sciences, California Institute of Technology, Pasadena, CA 91125, USA {ajtaylor, ames}@caltech.edu

³C. R. He is also with Plus.ai Inc., Cupertino, CA 95014, USA chaozhe.he@plus.ai

⁴G. Orosz is also with the Department of Civil and Environmental Engineering, University of Michigan, Ann Arbor, MI 48109, USA

swarms [7], autonomous aerial vehicles [8], robotic arms [9], robotic manipulators [10], quadrupedal robots [11], and bipedal robots [12], as well as simulation results on automotive systems [3], autonomous naval vehicles [13], and spacecraft [14]. The variety in this collection of results indicates that CBFs capture fundamental concepts underlying the notion of safety, irrespective of a specific domain, and suggests that CBFs are a valuable tool to consider in the process of modern control system design.

One of the appealing features of the CBF-based methodology for safety-critical control synthesis is the relatively intuitive nature of the theoretical safety guarantees they endow a system with. The study of *set invariance*, or the state of a system remaining within a prescribed set, has long been of interest in the study of dynamic systems [15] and control [16]. The foundational work in [17] proposed the notion of a *barrier function* as a tool for checking the invariance of a set given a model of the system dynamics. In simple terms¹, a barrier function takes positive values for states inside a set, and is zero on the boundary of the set. If the time derivative of the barrier function is positive on the boundary of the set, the value of barrier must grow and the system thus must remain in the set. This idea was quickly adapted to the context of control synthesis, yielding CBFs and a means to constructively achieve set invariance. Synthesis was first proposed through structured controllers [19], but was later expanded using convex optimization to produce *safety-filters* that minimally modify a hand-designed controller to ensure safety [1], [3], [4]. The combination of intuitive theoretical concepts with relatively simple control synthesis techniques promoted rapid development of CBFs, including formulations for higher-order systems [20]–[22] and discrete-time systems [23], as well as constructive tools for synthesizing CBFs [24]–[26] and methods for sets with complex geometries [27], [28].

Inherent in the theoretical safety guarantees provided by CBFs is a dependence on the model of the system dynamics, thus raising subsequent questions of robustness. Resulting works have explored robustness to disturbances [29]–[35], measurement errors [36], unmodeled dynamics [37], and sector-bounded uncertainties [38]. The early work in [29] noticed a robustness to disturbances inherent in CBFs, which drawing inspiration from the notion of Input-to-State Stability frequently seen when considering robust stabilization of nonlinear systems [39], was formalized into the idea of *Input-to-State Safety* (ISSf) in [32]. Instead of trying to keep a specific

¹We recommend the reader to [18] for a comprehensive mathematical study of the connections between barrier functions and set invariance.

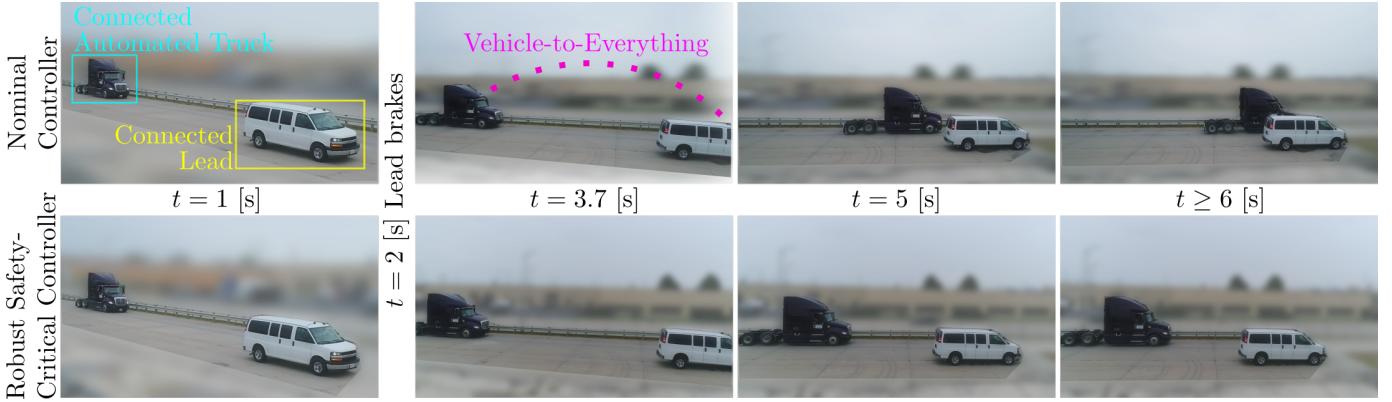


Fig. 1. Experimental configuration for heavy-duty CAV problem. (Top) Controller design without robustifying element yields safety violation and collision. (Bottom) Robust safety-critical controller ensures CAV brakes early and aggressively enough to maintain safe distance.

set invariant in the presence of disturbances as in [30], [31], which may induce conservativeness and degrade the performance of a controller, ISSf quantifies how the set kept invariant grows in the presence of disturbances. Moreover, it provides a simple modification for CBF-based controllers to control this growth, which was extended in [34] to permit greater performance while maintaining meaningful safety guarantees. As we demonstrate in this work, this paradigm for robust safety naturally lends itself to the design-test-redesign process, as the growth of the invariant set can be tuned to satisfy safety requirements while meeting performance metrics.

Despite the fact that CBFs were initially presented as a tool for safety-critical control synthesis for automotive systems [3], [29], they have yet to be experimentally realized on them. A primary challenge in using CBFs to ensure safety for a complex system such as a full-scale *connected automated vehicle* (CAV) lies in addressing discrepancies between the system model and the real-world system. In the context of a heavy-duty CAV, a significant portion of these discrepancies arise due to simplified models of the complex interactions within the CAV braking elements [40], and manifest as disturbances in the input applied to the system. Accounting for these complicated interactions in the controller design may greatly increase the intricacy of the resulting controller, but completely ignoring them may yield safety violations under critical conditions such as a harsh brake from a preceding vehicle as seen in Fig. 1 (top). Thus, balancing the complexity of the model used in design with the need to satisfy safety requirements is a challenging yet appropriate setting to deploy robust CBF-based control design.

There are two main contributions in this paper. The first is a tutorial presentation of a robust safety-critical design methodology using CBFs and ISSf. Concepts are introduced in parallel with an inverted pendulum example, thus providing a concrete context for readers to quickly establish an understanding of the relevant details in safety-critical control synthesis. We provide an appropriate level of theoretical discussion to clearly state the theoretical safety guarantees achieved with this control paradigm, but focus predominantly on the practical challenges and trade-offs encountered in safety-critical control design. Compared to the original works [3], [4] and overview

work [5] on CBFs, we believe that this presentation provides a more approachable introduction to the topic of safety-critical control synthesis for practitioners. Moreover, all details necessary to exactly recreate the simulation results in the inverted pendulum example are provided.

The second contribution of this work is a more practical application of the presented safety-critical control design methodology that considers a heavy-duty CAV, seen in Figure 1. We highlight the entire process of safety-critical control design including system modeling, specification of safety requirements via a CBF, nominal performance-based controller design, simulation, and experimental testing on a full-scale automated class-8 tractor. The impacts of unmodeled disturbances seen in experimental results are quantified and used to robustify the safety-critical controller, which is subsequently implemented in simulation and experimentally. We believe that combined tutorial presentation and the proposed design-test-redesign process on a challenging real-world system is precisely the approach necessary to advance CBF-based control design from the academic setting to a tool useful for the practicing control engineer.

The organization of this paper is as follows. In Section II we present the safety-critical control problem, review CBFs, and explore how a nominal controller may be modified via CBFs to endow a system with theoretical safety guarantees. In Section III we introduce disturbances into the input to the system, and explore how these impact theoretical safety guarantees through the lens of ISSf. Moreover, we present a simple framework for robustly modifying a CBF and the resulting controller design to provide a measure of control over how these safety guarantees degrade. In Section IV the connected automated vehicle problem is presented considering an automated heavy-duty vehicle. A CBF specified to encode safety for the CAV and a hand-designed nominal controller are incorporated into a safety-critical controller that is evaluated in simulation and verified to ensure safety. In Section V we deploy the controller experimentally, and see how unmodeled disturbances lead to degradation of safety guarantees. We characterize these disturbances and robustify the controller design, and lastly verify the ability of this controller to meet safety requirements both in simulation and experiments.

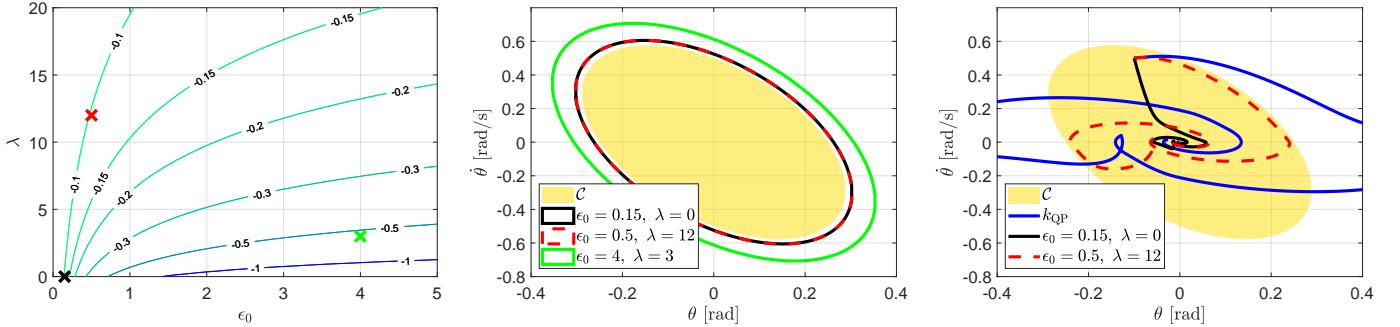


Fig. 7. (Left) Curves corresponding to the value of h^* solving (38) across the (ϵ_0, λ) parameter space for the inverted pendulum example. (Center) The boundary of the set C_δ rendered forward invariant for different choices of the parameters ϵ_0 and λ for the inverted pendulum example. Note that the C_δ contains the set C for each parameter set. (Right) Simulation results for the inverted pendulum system with disturbances. The gold ellipse is the safe set C defined in (8). The blue line is the trajectory of the system evolving under k_{QP} defined in (21)-(22), which is not robust to disturbances and leaves the safe set. The black and dashed red lines are the trajectory of the system evolving under \bar{k}_{QP} defined in (42)-(43) with different values for ϵ_0 and λ . While both parameter sets yield the same forward invariant set C_δ , the red parameter set is less conservative and allows the system to approach the boundary.

IV. SAFETY-CRITICAL CONTROLLER DESIGN FOR A CONNECTED AUTOMATED TRUCK

In this section, we go through the process of designing a safety-critical longitudinal controller for a connected automated truck. We first introduce the physical system and define a safe set via a Control Barrier Function. We then present a nominal performance-based controller, and synthesize a safety-critical controller that modifies this nominal controller in a minimally invasive way while ensuring safety.

A. Modeling Longitudinal Dynamics

In this work we consider a rear-axle-driven truck without a trailer. Assuming the truck's tires roll without slipping and the truck travels on a flat road with no headwind, the longitudinal dynamics of the truck are described by the following model:

$$\dot{v} = \frac{T}{m_{\text{eff}} R} - \frac{kv^2 + mg\gamma}{m_{\text{eff}}}. \quad (44)$$

Here the state is given by the truck's longitudinal speed $v \in \mathbb{R}$, the input is the torque applied on the rear axle $T \in \mathbb{R}$, and the parameters in the model are the mass of the truck m , the mass moment of inertia of the rotating elements I , the tire radius R , the effective mass $m_{\text{eff}} = m + \frac{I}{R^2}$, the air drag constant k , gravitational acceleration g , and rolling resistance coefficient γ . Note that the second term in (44) is dissipative in nature, and slows down the vehicle when it has a positive velocity. This term may be directly accounted for in the control design through via feedback linearization techniques [43], or may be ignored as its omission simply introduces a factor of conservativeness to the controller in terms of safety. The torque input commanded of the system is computed from a desired longitudinal acceleration command $u \in \mathbb{R}$ via feed-forward maps. This torque input command is provided by a drive-by-wire system to the low-level power generation systems that produce the actual torque T ; see Fig. 8. With these feed-forward maps in mind, we may simplify the model of the longitudinal dynamics of the truck to:

$$\dot{v} = u. \quad (45)$$

Now let us consider the scenario when the truck follows a connected vehicle as depicted in Fig. 8. Using the truck model in (45), the dynamics of this connected system are given by:

$$\begin{aligned} \dot{D} &= v_L - v, \\ \dot{v} &= u, \\ \dot{v}_L &= a_L, \end{aligned} \quad (46)$$

where $v_L, a_L \in \mathbb{R}$ are the speed and acceleration of the leading vehicle, respectively, and $D \in \mathbb{R}$ denotes the bumper-to-bumper headway distance between the truck and the lead vehicle, yielding the state $\mathbf{x} = [D, v, v_L]^\top \in \mathbb{R}^3$. The truck and lead vehicle are outfitted with vehicle-to-vehicle (V2V) communication systems, permitting the truck to receive motion information from the lead vehicle such as its GPS position which yields the distance D , its speed v_L , and its acceleration a_L . We assume that the leader's behavior satisfies:

$$a_L \in [-\underline{a}_L, \bar{a}_L], \quad v_L \in [0, \bar{v}_L], \quad (47)$$

where the parameters $\underline{a}_L, \bar{a}_L, \bar{v}_L > 0$ reflect a city-driving scenario; see Table II.

B. Safety and Control Barrier Function

The safety task for the truck is to maintain a safe distance behind the leader. This task motivates a Control Barrier

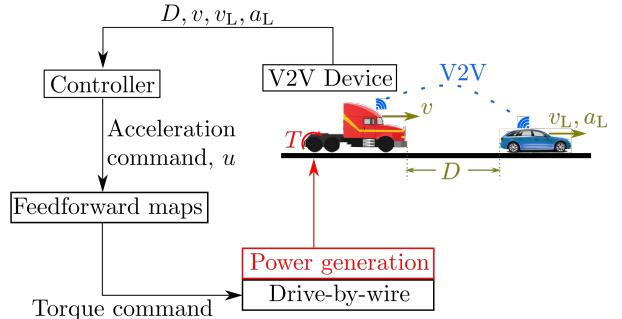


Fig. 8. A connected automated truck following a connected vehicle.

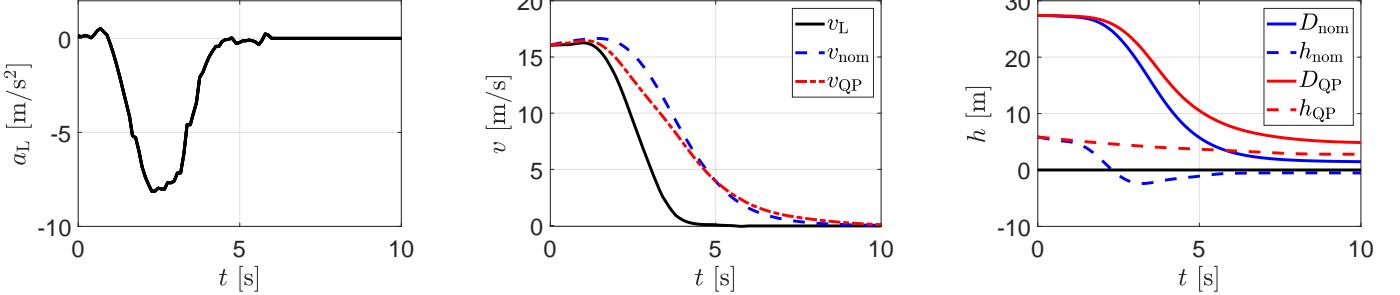


Fig. 12. (Left) Example profile for acceleration a_L of lead vehicle used in numerical simulation. (Center) Velocity v_L of lead vehicle (black) and velocity of the truck using the nominal controller (53) (blue) and safety-critical controller (57) (red). (Right) Following distance D and value of CBF h using the nominal controller and safety-critical controller.

Having designed the CBF h and the performance based nominal controller k_n , we can unify them via the safety-critical controller formulation for single input systems given in (21)-(22). Here we have:

$$\begin{aligned} L_f h(D, v, v_L) &= v_L - v - a_L(c_2 + c_4 v + 2c_5 v_L), \\ L_g h(D, v, v_L) &= -c_1 - 2c_3 v - c_4 v_L, \end{aligned} \quad (56)$$

where $L_g h(D, v, v_L) < 0$ for $v \geq 0$ and $v_L \in [0, \bar{v}_L]$. Then one may utilize the switch structure (22):

$$k_{QP}(D, v, v_L) = \min \{k_n(D, v, v_L), k_s(D, v, v_L)\}, \quad (57)$$

where the second term is defined as:

$$k_s(D, v, v_L) = -\frac{L_f h(D, v, v_L) + \alpha_c h(D, v, v_L)}{L_g h(D, v, v_L)}. \quad (58)$$

This controller utilizes the nominal controller k_n to optimize the performance when it is safe. Otherwise, the provably safe controller k_s becomes smaller than k_n and intervenes to ensure safety. Note that $L_g h(D, v, v_L) > 0$ for sufficiently large $v_L > \bar{v}_L$ (as c_4 is negative) as well as sufficiently negative $v < 0$, yielding the switch structure (21), but this is outside the domain of interest in this application.

We simulate both the nominal controller and safety-critical controller via numerical integration of the model (46) from the initial condition $\mathbf{x}(0) = [27.4, 16, 16]^\top \in \mathcal{C}$. We use parameter values as specified in Table II. The acceleration a_L of the lead vehicle is given by a time profile reflecting a hard braking event, as seen in Fig. 12 (left). The velocity of the truck converges to zero and a crash does not occur for both controllers, but only the safety-critical controller ensures the truck maintains a safe distance (indicated by $h_{QP}(\mathbf{x}(t)) \geq 0$) as seen in Fig. 12 (center, right). We see that the nominal controller brakes less aggressively than the safety-critical controller, and thus does not react quickly enough to avoid violating the safe following distance requirement.

V. EXPERIMENTAL RESULTS & ROBUST DESIGN

In this section we provide a description of the automated truck experimental configuration and present results using the nominal and safety-critical controllers. Furthermore, we deploy the method of robust control design using ISSf developed in Section III, and demonstrate its advantages experimentally.

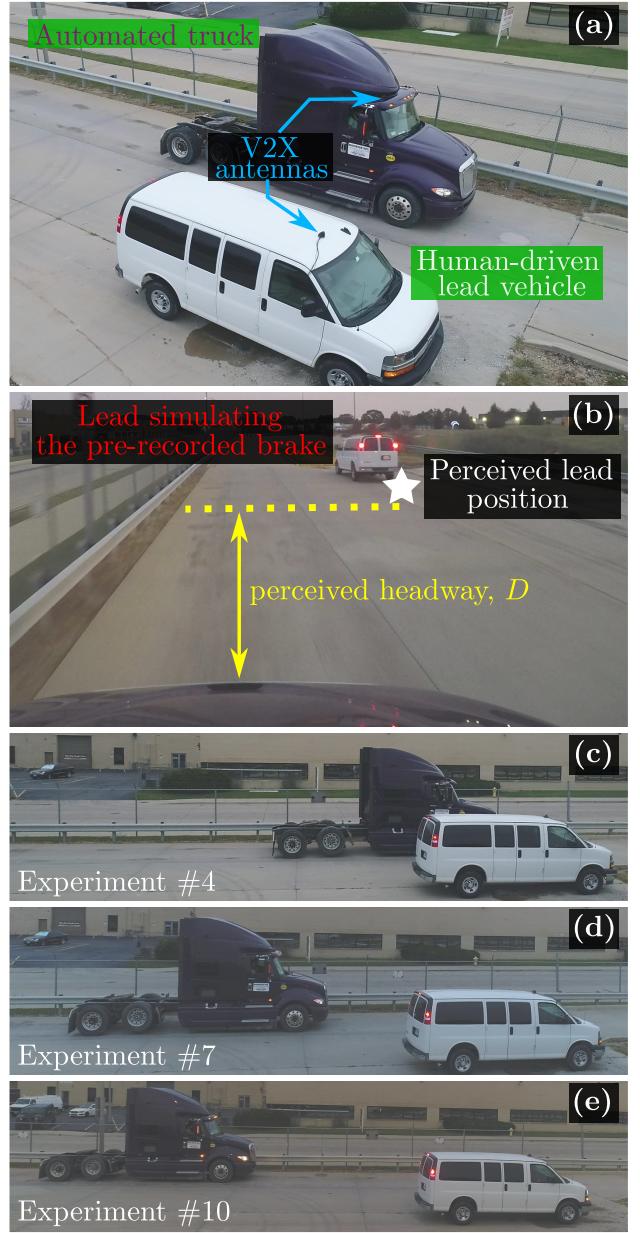


Fig. 13. (a) Vehicles used in experiments. (b) Image from the dashboard of the truck during an experimental run. (c,d,e) Final configurations of separate experiments. See [49] for a video.

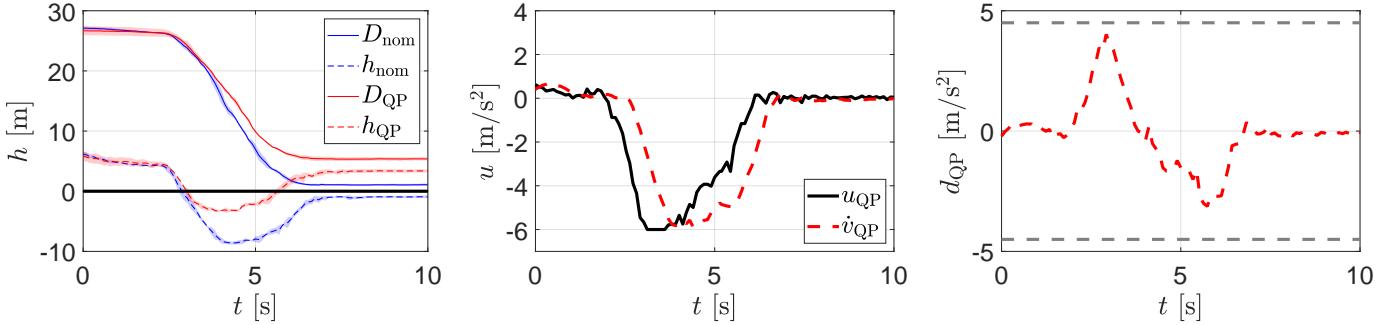


Fig. 14. (Left) Mean value (lines) and standard deviations (fills) of the distance D and the CBF h when using the nominal controller defined in (53) (blue) and the safety-critical controller defined in (57) (red) in the truck experiment. The repeated experiments with these controllers are highly consistent. (Center) Discrepancy between acceleration commanded by safety-critical controller (black) and actual acceleration of the automated truck (red). (Right) Disturbance signal in input seen by the truck used to define the model (59).

A. Experimental Setup and Procedure

The automated truck used in our experiments is an International ProStar+ Class-8 truck developed by the Navistar [50]; see Fig. 13(a). Both the automated truck and the lead vehicle are equipped with a V2X Onboard Unit (OBU) developed by Commsignia [51]. These units are equipped with an accelerometer, gyroscope, magnetometer, and GPS unit. Furthermore, these OBUs support peer-to-peer communication such that the automated truck may receive position, velocity, and acceleration data from the lead vehicle through V2X antennas shown in Fig. 13(a). The automated truck is additionally equipped with a Mobile Real-Time Targeting Machine developed by Speedgoat [52], which interfaces with the V2X OBU and the truck's Engine Controller Unit (ECU) through a Controller Area Network (CAN) bus. The Speedgoat runs the controller for the system given a measurement stream of values for D , v , v_L , and a_L coming from the V2X OBUs. It computes a desired acceleration input and converts it to a corresponding torque value through a feed-forward map. A drive-by-wire system on the truck controls the engine and the brake torques accordingly. The steering of the truck is done manually by a human driver in the experiments.

In an effort to evaluate the repeatability of our experiments, it is necessary to eliminate variation in the lead vehicle's behavior, which is being driven by a human. To achieve this, we use a pre-recorded time profile of position, velocity, and acceleration of the lead vehicle while it performs a hard braking event. This profile for a_L and v_L is seen in the left and center panels of Fig. 12, and was used to produce our simulation results. We stream this data to the truck controller as the *perceived lead vehicle* in our experiments. Experiments also include a physical lead vehicle simulating the pre-recorded motion for visualization purposes; see Fig. 13(b). Importantly, the evaluation of safety is derived from evaluating the CBF using the recorded time profiles rather than simply detecting collisions such as Fig. 13(c). A video of the experiments are available online [49].

B. Input Disturbances

We deploy both the nominal and safety-critical controller on the automated truck with results as seen in the left panel

of Fig. 14. We see that not only does the nominal controller consistently fails to meet the safety requirements imposed by the CBF h , but the safety-critical controller also consistently fails to meet the safety requirements. The top row in Fig. 1 illustrates an experimental run with the nominal controller.

To understand why the safety-critical controller fails, we examine the discrepancy between the commanded acceleration and actual acceleration of the automated truck, as seen in the center panel of Fig. 14. One may observe a delay between the commanded acceleration and the achieved acceleration. This delay in acceleration is due to the fact that the power generation of the truck is a complex nonlinear dynamical system that has been imperfectly abstracted away by the feed-forward maps that allow the simplified model in (45). Rather than attempting to work with this complex nonlinear dynamic system and improving the feed-forward maps, we describe the discrepancy in commanded and actual acceleration as a disturbance in the simplified model:

$$\dot{v} = u + d(t), \quad (59)$$

where $d : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$ reflects the difference between commanded acceleration and actual acceleration.

As the disturbance d is caused by the complicated interactions of the drive-by-wire system and power generation dynamics, it may be difficult to use model-based techniques to construct a meaningful bound δ for the worst-case disturbance. Instead, we estimate the worst-case disturbance empirically by comparing the actual acceleration $\dot{v}(t)$ to the commanded acceleration $u(t)$. In the right panel of Fig. 14, we see that the largest difference in the commanded and actual acceleration is around 4 [m/s^2]. Thus, we study the degradation of safety of the system taking a slightly larger value $\delta = 4.5$ [m/s^2].

C. Robust Design

To overcome this disturbance and improve the safe behavior of the truck, we deploy the tools of ISSf-CBFs described in Section III. As h satisfies the CBF condition (10), it also satisfies the ISSf-CBF condition (31), where we take:

$$\epsilon(r) = \epsilon_0 e^{\lambda r}, \quad (60)$$

with $\epsilon_0 > 0$ and $\lambda \geq 0$. The parameter λ introduces a measure of flexibility by allowing one to require a greater degree of

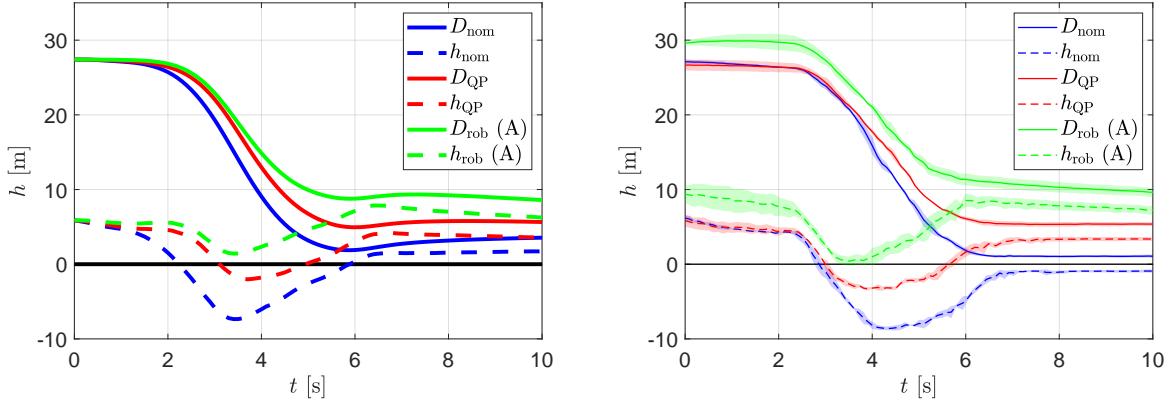


Fig. 15. (Left) Following distance and value of ISSf-CBF using the nominal controller (blue), safety-critical controller (red), and robust safety-critical controller (green) in the disturbed simulation. (Right) Mean value (lines) and standard deviations (fills) of the distance D and the ISSf-CBF h using the nominal controller (blue), safety-critical controller (red), and robust safety-critical controller (green) in experiment.

robustness when the truck is close to the leading vehicle, and less robustness when the distance is greater. Given (60), the forward invariant set is given by:

$$\mathcal{C}_\delta = \left\{ \begin{bmatrix} D \\ v \\ v_L \end{bmatrix} \in \mathbb{R}^3 \mid h(D, v, v_L) \geq -\frac{\epsilon_0 e^{\lambda h(D, v, v_L)} \delta^2}{4\alpha_c} \right\}. \quad (61)$$

As discussed in the inverted pendulum example, the set \mathcal{C}_δ being forward invariant implies that $h(\mathbf{x}(t)) \geq h^*$, where h^* is the value of the ISSf-CBF h on the boundary of \mathcal{C}_δ , which can be calculated by solving (35). The value of h^* for different choices of ϵ_0 and λ can be seen in Table III. We then construct an optimization-based controller giving the switch structure (43), since $L_g h(D, v, v_L) < 0$ for $v \geq 0$ and $v_L \in [0, \bar{v}_L]$ (cf. (56)). This results in:

$$k_{\text{rob}}(D, v, v_L) = \min \{ k_n(D, v, v_L), \bar{k}_s(D, v, v_L) \}, \quad (62)$$

where:

$$\bar{k}_s(D, v, v_L) = k_s(D, v, v_L) + \frac{L_g h(D, v, v_L)}{\epsilon_0 e^{\lambda h(D, v, v_L)}}, \quad (63)$$

and k_n and k_s are given by (53) and (58), respectively.

We simulate the nominal controller, safety-critical controller, and robust safety-critical controller via numerical integration of the model (46) from the initial condition $\mathbf{x}(0) = [27.4, 16, 16]^\top \in \mathcal{C}$ while disturbing the input using the signal in shown in the right panel of Fig. 14. We use parameter values as specified in Table II. We see in the left panel of Fig. 15 that introducing the disturbance signal into our simulation allows us to recreate the failures of the nominal controller and safety-critical controller that we saw experimentally in Fig. 14. Furthermore, we see that the robust safety-critical controller maintains the safety of the system even in the presence of the disturbance.

D. Robust Experimental Results

Here we show the results when the robust safety-critical controller is deployed on the connected automated truck. Sets of three experimental runs were conducted using each parameter pair ϵ_0 and λ shown in Table III. The experimental results

using the parameter set $\epsilon_0 = 0.5$ [s^3/m] and $\lambda = 0.4$ [$1/\text{m}$] (labeled as parameter pair (A)) can be seen in the right panel of Fig. 15 and are visualized at the bottom row of Fig. 1. With these parameters the system is rendered safe, as the value of h does not drop below 0. Although the robust safety-critical controller displays a larger standard deviation across the three experimental runs compared to the nominal and safety-critical controllers, it consistently satisfies the original safety requirement.

When evaluating how the system behavior depends on the values of the parameters ϵ_0 and λ , we first consider whether the original safety requirement is met, i.e., whether or not the value of h remains positive. While the robust-safety critical controller does not provide a theoretical guarantee that h will remain non-negative (it only guarantees that $h(\mathbf{x}(t)) \geq h^*$), for certain values of ϵ_0 and λ the original safety requirement are still met, as seen in the inverted pendulum example as well as the connected automated truck experiments. The minimum value h_{\min} of the barrier function, observed during the experimental runs, is shown in Table III. This is also visualized in the left panel of Fig. 16, where green markers indicate sets of parameter values for which the safety requirement is met, and red markers indicate those for which it is not met. We see that safety can be achieved using the original ISSf-CBF

Label	ϵ_0 [s^3/m]	λ [$1/\text{m}$]	h^* [m]	h_{\min} [m]	\tilde{D}_{ss} [m]
(B)	0.8	0	-40.50	22.09	25.43
	3	0	-151.88	2.99	6.19
(D)	4	0	-202.50	1.02	4.69
	5	0	-253.13	-0.45	3.54
(A)	0.5	0.4	-4.38	0.35	4.70
	0.5	0.5	-3.80	-1.27	2.22
(C)	0.8	0.25	-7.01	0.78	4.34
	0.8	0.35	-5.64	-1.03	2.22
	1.0	0.25	-7.59	-0.86	3.07

TABLE III. Sets of parameter values used for the exponential function (60) in the automated truck experiments with theoretical safety guarantee h^* , minimum experimental value of the ISSf-CBF h_{\min} , and shift in the steady-state tracking distance \tilde{D}_{ss} by (64).

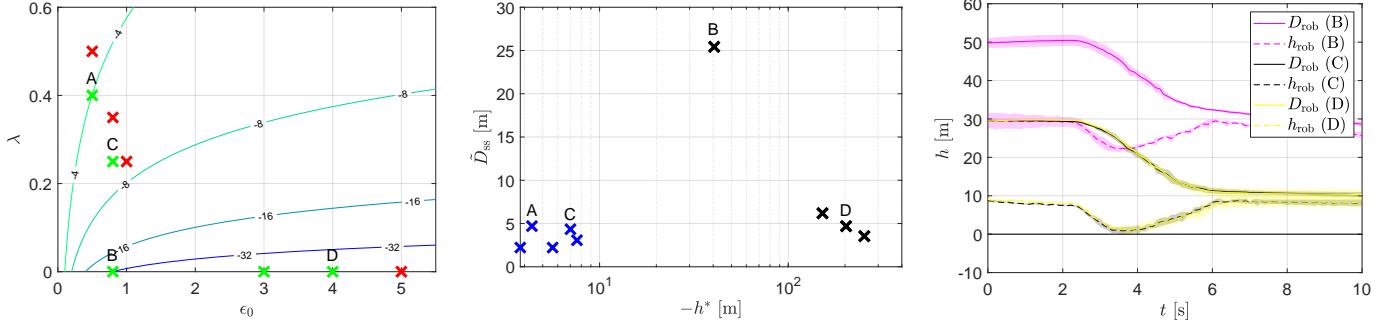


Fig. 16. (Left) Parameter values for ϵ_0 and λ used in the truck experiments, with contours showing theoretical values of h^* . Green markers denote parameter sets which achieve the original safety goal ($h \geq 0$), while red markers denote parameter sets for which the original safety goal is violated. (Center) Theoretical values of h^* and the shift in steady-state tracking distance, denoted by \tilde{D}_{ss} , for the parameter sets used in the truck experiments. The blue markers denote parameter sets with $\lambda > 0$, while the black markers denote parameter sets with $\lambda = 0$. (Right) Experimental results for parameter pairs (B), (C) and (D) in Table III. Case (B) is highly conservative as indicated by the large steady-state tracking distance error. Cases (C) and (D) display nearly identical behavior, though case (C) possesses a much stronger theoretical guarantee.

formulation in [32] (where $\lambda = 0$) for sufficiently small values of ϵ_0 , but may also be achieved using small values of λ .

We remark that when changing the controller from k_{QP} (cf. (57)) to k_{rob} (cf. (62)) the equilibrium of the system is shifted as can be noticed once comparing the runs on the right panel of Fig. 15. We characterize this by the shift in the steady-state tracking distance error defined as

$$\tilde{D}_{ss} \triangleq D_{ss}^{\text{exp}} - D^*. \quad (64)$$

Here D_{ss}^{exp} is the steady-state distance captured in experiments when the leader is moving with the steady-state speed $v^* \in (0, \bar{v}_L)$ before braking. The term $D^* = V^{-1}(v^*)$ captures the desired steady-state distance given by the inverse of the range policy (54). In the experiments we have $v^* = 16$ [m/s], yielding $D^* = 25$ [m]. The values of \tilde{D}_{ss} corresponding to different parameter pairs are given in Table III. In the right panel of Fig. 16 we visualize the theoretical values of h^* and the experimental values of \tilde{D}_{ss} for different parameter sets. The black markers indicate parameter sets with $\lambda = 0$, while the blue markers show parameter sets with $\lambda > 0$. With $\lambda = 0$, the theoretical guarantees are nearly meaningless (observe the large negative values of h^*), and improving them requires dramatically increasing \tilde{D}_{ss} . In contrast, the parameter sets with $\lambda > 0$ allow us to obtain significantly (an order of magnitude) stronger theoretical guarantees without greatly increasing \tilde{D}_{ss} , thereby also achieve good performance. In the right panel of Fig. 14 we give experimental results of three other parameter pairs labeled as (B), (C) and (D) in Table III. The poor performance of case (B) is indicated by the large value of \tilde{D}_{ss} . The results for cases (C) and (D) nearly overlap, but the introduction of λ allows strong theoretical guarantee for case (C) which is missing for case (D).

VI. CONCLUSION

In conclusion, this work has developed a theoretically rigorous approach for safety-critical control synthesis through Control Barrier Functions (CBFs). The notion of Input-to-State Safety (ISSf) is utilized to capture the impact of disturbances in the input to the system. A simple parametric modification to

CBFs enabled the formulation of ISSf-CBFs as a practical tool for achieving both performant behavior and meaningful theoretical safety guarantees. We provided a tutorial on these tools in the context of an inverted pendulum system, and carried out a practical design problem of a safety-critical controller for a connected automated truck. Moreover, we demonstrated the tangible benefits of the design using ISSf-CBFs by deploying this controller experimentally on an automated truck.

APPENDIX

A. Proof of Theorem 2

Proof. We first prove that the optimization problem in (18) has a closed-form solution given by (19) and (20), thereby proving it is feasible for any $\mathbf{x} \in \mathbb{R}^n$ and satisfies $\mathbf{k}_{QP}(\mathbf{x}) \in K_{CBF}(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^n$. Then we prove that \mathbf{k}_{QP} is a continuous function.

Let us first consider an $\mathbf{x} \in \mathbb{R}^n$ such that $L_g h(\mathbf{x}) = \mathbf{0}$. By assumption, the function h is a CBF for (1) on the set \mathcal{C} with corresponding function $\alpha \in \mathcal{K}_\infty^e$. Thus, we know from the condition in (10) that

$$L_f h(\mathbf{x}) + \alpha(h(\mathbf{x})) > 0, \quad (65)$$

such that the inequality constraint in (18) is satisfied for any choice of \mathbf{u} . The definition of a norm requires that for any $\mathbf{y} \in \mathbb{R}^m$, we have $\|\mathbf{y}\|_2 \geq 0$ and $\|\mathbf{y}\|_2 = 0$ implies $\mathbf{y} = \mathbf{0}$. Thus, we may conclude that the minimizing choice of \mathbf{u} is given by $\mathbf{u} = \mathbf{k}_n(\mathbf{x})$, such that $\mathbf{k}_{QP}(\mathbf{x}) = \mathbf{k}_n(\mathbf{x})$ as required by the closed-form solution in (19) and (20).

Next let us consider an $\mathbf{x} \in \mathbb{R}^n$ such that $L_g h(\mathbf{x}) \neq \mathbf{0}$. Observe that the cost function and constraint function defining (18) are both convex and continuously differentiable with respect to the decision variable \mathbf{u} . Thus the optimization problem is convex, and the *Karush-Kuhn-Tucker* (KKT) conditions provide a necessary and sufficient³ condition for optimality [53, §5.5.3]. More precisely, the KKT conditions state that for

³An additional *constraint qualification* is necessary for the KKT conditions to be necessary and sufficient conditions for optimality. One such qualification is *Slater's Condition* [53, §5.2.3], which is easily verified to hold in our setting.

- [52] Speedgoat, “Mobile real-time target machine,” <https://www.speedgoat.com/products-services/real-time-target-machines/mobile>.
- [53] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge University Press, 2004.



Anil Alan received the BSc degree in mechanical engineering from Middle East Technical University, Turkey, in 2012 and the MSc degree in Bilkent University, Turkey, in 2017. He is currently pursuing the PhD degree in mechanical engineering with the University of Michigan, Ann Arbor, MI, USA. His current research interests include control of connected autonomous vehicles, safety-critical control, nonlinear control, vehicle dynamics.



Gábor Orosz received the M.Sc. degree in Engineering Physics from the Budapest University of Technology, Hungary, in 2002 and the Ph.D. degree in Engineering Mathematics from University of Bristol, UK, in 2006. He held postdoctoral positions at the University of Exeter, UK, and at the University of California, Santa Barbara. In 2010, he joined the University of Michigan, Ann Arbor where he is currently an Associate Professor in Mechanical Engineering and in Civil and Environmental Engineering. His research interests include nonlinear dynamics and control, time delay systems, and reinforcement learning with applications to connected and automated vehicles, traffic flow, and biological networks.



Andrew J. Taylor received the B.S. and M.S. degrees in aerospace engineering from the University of Michigan, Ann Arbor, in 2016 and 2017, respectively. He is currently pursuing a Ph.D. degree at California Institute of Technology in Control and Dynamical Systems. His research interests include safety-critical control for robotic systems and data-driven control techniques for nonlinear systems.



Chaozhe R. He received the BSc degree in applied mathematics from the Beijing University of Aeronautics and Astronautics in 2012, the MSc and PhD in Mechanical Engineering from the University of Michigan, Ann Arbor, USA, in 2015 and 2018 respectively. Dr. He is with Plus.ai Inc. and is working on planning and control algorithm development. His research interests include dynamics and control of connected automated vehicles, optimal and nonlinear control theory, and data-driven control.



Aaron D. Ames is the Bren Professor of Mechanical and Civil Engineering and Control and Dynamical Systems at Caltech. Prior to joining Caltech in 2017, he was an Associate Professor at Georgia Tech in the Woodruff School of Mechanical Engineering and the School of Electrical & Computer Engineering. He received a B.S. in Mechanical Engineering and a B.A. in Mathematics from the University of St. Thomas in 2001, and he received a M.A. in Mathematics and a Ph.D. in Electrical Engineering and Computer Sciences from UC Berkeley in 2006. He served as a Postdoctoral Scholar in Control and Dynamical Systems at Caltech from 2006 to 2008, and began his faculty career at Texas A&M University in 2008. At UC Berkeley, he was the recipient of the 2005 Leon O. Chua Award for achievement in nonlinear science and the 2006 Bernard Friedman Memorial Prize in Applied Mathematics, and he received the NSF CAREER award in 2010, the 2015 Donald P. Eckman Award, and the 2019 IEEE CSS Antonio Ruberti Young Researcher Prize. His research interests span the areas of robotics, nonlinear, safety-critical control and hybrid systems, with a special focus on applications to dynamic robots — both formally and through experimental validation.