Sample-and-Hold Safety with Control Barrier Functions

Gilbert Bahati, Pio Ong, and Aaron D. Ames

Abstract— A common assumption on the deployment of safeguarding controllers on the digital platform is that high sampling frequency translates to a small violation of safety. This paper investigates and formalizes this assumption through the lens of Input-to-State Safety. From this perspective, and leveraging control barrier functions (CBFs), we propose an alternative solution for maintaining safety of sample-and-hold control systems without any violation to the original safe set. Our approach centers around modulating the sampled control input in order to guarantee a more robust safety condition. We analyze both the time-triggered and the event-triggered sample-and-hold implementations, including the characterization of sampling frequency requirements and trigger conditions. We demonstrate the effectiveness of our approach in the context of adaptive cruise control through simulations.

I. INTRODUCTION

Safety-critical systems are a crucial part of a variety of application domains: transportation, manufacturing, healthcare among others. In such systems, the occurrence of safety violations, no matter how small, may lead to catastrophic consequences. In these systems, electronic devices are often used to implement digital control, where continuous signals from the real-world systems are sampled at regular intervals [1]. However, this can result in measurement uncertainties due to sampling (i.e., zero-order hold errors), which can lead to safety violations. Therefore, it is essential to design robust control methods that can account for these errors to guarantee safety. To mitigate these sample-and-hold errors, a common practice is to sample at high frequencies, limiting the error to a small and hopefully negligible value. However, this does not entirely eliminate the error, only reducing it to an acceptable level. It is often still the case that absolute safety (even in the presence of these errors) is desired.

To avoid dealing with the sample-and-hold error explicitly, it is common to consider a discrete time approximation [2] of the available continuous time system as done in sampled data systems [3]–[8]. However, obtaining these approximations can introduce additional error since the exact solutions to the continuous time systems are generally not known. Furthermore, discrete time designs explicitly guarantee safety only at sampling instants (when the controller is updated) and not in the inter-sample periods (when the control signal is being held constant) and as such, safety may be violated during this period. To formalize this property of discrete time approximations, the notion of practical safety [3] is usually adopted to account for these possible violations during the

inter-sample period. Practically safe systems can maintain their state within a safe set during sample times, provided that the sampling frequency is high enough. This results in safety being ensured with respect to a larger set that accommodates all possible violations of the original set.

The notion of safe set expansion to accommodate uncertainties in a system can be encapsulated by Input-to-State Safety (ISSf) [9]. In particular, this generalizes Input-to-State Stability (ISS) [10]–[12] in the context of safe sets, wherein disturbances in the input result in convergence to a region of the safe set dictated by the size of the disturbance. To certify ISSf, the framework of Control Barrier Functions (CBFs) [13]–[15] can be leveraged. In particular, the existence of an ISSf-CBF implies the system is ISSf. This notion was generalized in a "tunable" fashion in [16] allowing for more control over the expansion of the safe set—an extension that has found applications in practice [17], [18]. Yet obtaining safety guarantees in the context of CBFs does not address digital implementation issues raised by sample-and-hold.

There is a rich body of work on translating discretely instantiated continuous-time systems in a way that preserves desired properties, encapsulated by the area of event-triggered control [19], [20]. This has historically studied stability, and used Lyapunov functions to quantify when to sample and hold to guarantee that stability is maintained: the result are Lyapunov-based trigger laws that utilize ISS to bound the system behavior during the inter-sample periods [19]. Event-triggered control has also been studied in the context of safety using CBFs [21]–[24], wherein safety during inter-sample periods is guaranteed for specific systems [21] or through codesign approaches limited to specific controllers [22], [23]. Typically, if nominal controllers do not satisfy the characterized conditions of robustness, safety relies on expanding the safe set to accommodate inter-sample errors [24], resulting in small safety violations similar to those seen in the sample-and-hold framework.

The main contribution of this paper is a robust control framework for sample-and-hold control systems that establishes safety without violations or relaxations of the safe set of interest. We achieve this by mathematically formalizing the notion of practical safety [3] through the Input-to-State Safety (ISSf) framework [9]. In particular, we present a modulation of the nominal controller that guarantees safety on the original safe set without resorting to expansions of the set. Similar nominal controller adjustments have been proposed in the literature to provide ISSf guarantees to a system [9], [16] with respect to some disturbances; however, these approaches have not been utilized in the context of mitigating disturbances from sample-and-hold errors, where

a coupling exists between the controller adjustment and the disturbance. Furthermore, to mitigate the conservative nature of the proposed designs, we leverage the event-triggered control approach [19], [24] to synthesize controllers that address such conservatism yet still maintain robustness to sample-and-hold errors. In short, the main result guarantees the safety (forward invariance) of the original safe set—attenuating conservatism while ensuring inter-sample safety.

Notation: We utilize $\mathbb{N}$, $\mathbb{R}$, $\mathbb{R}_{\geq 0}$, $\mathbb{R}_{>0}$ to denote natural, real, nonnegative, and positive numbers, respectively. For a vector $x \in \mathbb{R}^n$, $\|x\|$ denotes the Euclidean norm and $\|x\|_\mathcal{C} = \inf\{\|x - y\| \mid y \in \mathcal{C}\}$ is its Hausdorff distance to set $\mathcal{C}$. Then given a set $\mathcal{C}$, a δ-neighborhood of $\mathcal{C}$ is the set $\{x \mid \|x\|_\mathcal{C} < \delta\}$. A function $\alpha : [0, a) \to \mathbb{R}_{\geq 0}$ with $a > 0$, is of class-$\mathcal{K}_\infty$ if $\alpha(0) = 0$, α is strictly increasing, and $\lim_{s \to \infty} \alpha(s) = \infty$. A function $\beta : [-b, a) \to \mathbb{R}$ is of class-$\mathcal{K}_\infty^e$ if it is of class-$\mathcal{K}_\infty$ and $\beta(y) \leq 0$ for all $y \in [-b, 0]$.

II. SAFETY FOR CONTINUOUS-TIME SYSTEMS

This section provides the background on barrier functions and its usage for guaranteeing safety for continuous-time systems. In addition, we will review the robustness concept in safety within the construct of Input-to-State Safety.

Safety For Continuous Time Systems: We consider the nonlinear system:

$$\dot{x} = F(x, u), \tag{1}$$

where $x \in \mathbb{R}^n$ is the state and $u \in \mathbb{R}^m$ is the input. The system vector field $F : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is assumed to be locally Lipschitz. The goal of safety is to maintain all system trajectories within a *safe set* $\mathcal{C} \subset \mathbb{R}^n$. In other words, we want the set $\mathcal{C}$ to be forward invariant.

Definition 1. *(Safety):* A set $\mathcal{C}$ is forward invariant if for every initial condition $x_0 \in \mathcal{C}$, its ensuing trajectory $x(t) \in \mathcal{C}$ $\forall t \geq 0$. A system is safe on $\mathcal{C}$ if the set $\mathcal{C}$ is forward invariant. ●

One approach to guaranteeing safety is to describe a given set $\mathcal{C}$ with a continuously differentiable *barrier function* $h : \mathbb{R}^n \to \mathbb{R}$ such that:

$$\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}, \tag{2a}$$

$$\partial\mathcal{C} = \{x \in \mathbb{R}^n : h(x) = 0\}, \tag{2b}$$

$$\mathrm{Int}(\mathcal{C}) = \{x \in \mathbb{R}^n : h(x) > 0\}. \tag{2c}$$

In this case, the set $\mathcal{C}$ is the 0-superlevel set of the barrier function h, and the safety goal is then to keep the function h positive at all times. This can be achieved by designing a Lipschitz continuous controller $k : \mathbb{R}^n \to \mathbb{R}^m$ so that the state feedback $u = k(x)$ satisfies the *barrier condition* [13]:

$$\frac{\partial h}{\partial x}(x)F(x, k(x)) \geq -\alpha(h(x)), \tag{3}$$

for some class-$\mathcal{K}_\infty^e$ function α. When the above condition is met, we call the controller k a *safeguarding controller* that renders the system safe on $\mathcal{C}$.

The barrier condition provides a conservative approach for achieving safety. In addition to making sure that on the

boundary of the safe set, the vector field of the closed-loop system points towards the interior of the set (cf., Nagumo's Theorem [25]), the condition also limits the speed at which the trajectories may approach the boundary $\partial\mathcal{C}$. One benefit of this approach is the ability to formulate robustness through the notion of Input-to-State Safety, which we discuss next.

Safety Robustness: In the presence of disturbances added to the system, a safeguarding controller may fail to render the system safe on the safe set $\mathcal{C}$. In such cases, we may want the system trajectories to at least stay close to the safe set. One mathematical framework for guaranteeing such a behavior is Input-to-State Safety[1].

Consider the closed-loop nonlinear control-affine system with disturbance:

$$\dot{x} = F_e(x, k(x), e), \tag{4}$$

where $e \in \mathbb{R}^{n_e}$ is a bounded disturbance. We assume $F_e : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^{n_e} \to \mathbb{R}^n$ is locally Lipschitz in the state and control, and continuous in disturbance. Input-to-State Safety seeks to establish a relationship between the maximum size that the disturbance signal $t \mapsto e(t)$ achieved along the trajectory (i.e., $\|e\|_\infty$), and how far the trajectory may stray away from the safe set. Given a safe set $\mathcal{C}$, we use the barrier function h as a proxy to define a larger set $\mathcal{C}_e \supset \mathcal{C}$ as:

$$\mathcal{C}_e = \{x \in \mathbb{R}^n : h(x) + \gamma(\|e\|_\infty) \geq 0\}, \tag{5a}$$

$$\partial\mathcal{C}_e = \{x \in \mathbb{R}^n : h(x) + \gamma(\|e\|_\infty) = 0\}, \tag{5b}$$

$$\mathrm{Int}(\mathcal{C}_e) = \{x \in \mathbb{R}^n : h(x) + \gamma(\|e\|_\infty) > 0\}, \tag{5c}$$

where γ is a class-$\mathcal{K}_\infty$ function.

Definition 2. *(Input-to-State Safety):* A system is Input-to-State Safe (ISSf) on $\mathcal{C}$ if there exists a function $\gamma \in \mathcal{K}_\infty$ such that it is safe on $\mathcal{C}_e$ under any disturbance signal $t \mapsto e(t)$. ●

The existence of a function γ, and therefore Input-to-State Safety on set $\mathcal{C}$, can be established if the following *Input-to-State Safe barrier condition* (ISSf-BC) [9] holds:

$$\frac{\partial h}{\partial x}(x)F_e(x, k(x), e) \geq -\alpha(h(x)) - \iota(\|e\|) \tag{6}$$

for some class-$\mathcal{K}_\infty$ function ι.

III. PRACTICAL SAFETY FROM ISSF PERSPECTIVE

We focus on discretely instantiated continuous-time systems that result from sample-and-hold (i.e., zero-order hold) implementations of safeguarding controllers on digital platforms, and examine potential safety issues that arise. We limit ourselves to control-affine systems:

$$\dot{x} = f(x) + g(x)u, \tag{7}$$

where the system vector fields $f : \mathbb{R}^n \to \mathbb{R}^n$ and $g : \mathbb{R}^n \to \mathbb{R}^{n \times m}$ are assumed to be locally Lipschitz.

Given a nominal controller $k_{\mathrm{nom}} : \mathbb{R}^n \to \mathbb{R}^m$, the sample-and-hold implementation strategy is as follows: the controller is sampled at a time instant t_i, then the control value $u =$

---

[1]Sometimes more precisely as Disturbance-Input-to-State Safety

$k_{\text{nom}}(x(t_i))$ is held constant until t_{i+1}, the next sampling instant. As a result, the closed-loop system is given by:

$$\dot{x} = f(x) + g(x)k_{\text{nom}}(x + e) \quad \forall t \in [t_i, t_{i+1}), \quad (8)$$

with a sample-and-hold error $e = x(t_i) - x$. Due to the presence of this sample-and-hold error, the safeguarding nominal controller may not be able to fulfill its safety task, i.e., rendering the sample-and-hold system (8) safe on $\mathcal{C}$.

A. Practical Safety

In practice, a typical approach for dealing with sample-and-hold errors is through high frequency sampling, relying on the idea referred to as *practical safety* [3]. A system is deemed practically safe if the states (along the trajectories starting from $\mathcal{C}$), can be maintained at a distance arbitrarily close to the original safe set $\mathcal{C}$, with a sufficiently high sampling frequency, i.e., violations of safety appear to be minor if we sample fast enough, as illustrated in Fig. 1(a).

Although the description of practical safety seems reasonable, it is quite difficult to show that a controller yields practical safety. To this end, the usual argument for practical safety is that of Input-to-State safety (ISSf) discussed in Section II. The idea is based on two key reasonable assumptions:

- **Minor Safety Violations:** Small errors e should only lead to minor violations of safety of $\mathcal{C}$.
- **Small Error Bounds:** Under high frequency sampling, the error e should not be able to grow too large.

Although these concepts are often cited as the reasons for practical safety, to the best of our knowledge, no mathematical formalization of them exists. In the subsequent section, we develop a set of assumptions that enable us to use ISSf as a basis for practical safety.

B. Minor Safety Violations

Practical safety and Input-to-State Safety (ISSf) both acknowledge the fact that the presence of disturbances in a system may harm the safety guarantees provided by a controller. Furthermore, both aim to characterize safety violations as an increasing function of the size of disturbances. However, the two concepts are not exactly the same. ISSf describes safety violations with superlevel sets of barrier functions rather than generally with any set expansion. On the other hand, practical safety particularly deals with set expansions arising from the effect of sample-and-hold errors. Nevertheless, there is a great overlap between the two concepts, and our work lies at their intersection. Specifically, we consider when the nominal controller is a safeguarding controller satisfying the barrier condition (2) for the nominal system (7) as:

$$\underbrace{\frac{\partial h}{\partial x}(x)f(x)}_{\mathcal{L}_f h(x)} + \underbrace{\frac{\partial h}{\partial x}(x)g(x)}_{\mathcal{L}_g h(x)} k_{\text{nom}}(x) \geq -\alpha(h(x)).$$

However, the evolution of the barrier function along the trajectory of the sample-and-hold system (8) is given by:

$$\dot{h}(x, k_{\text{nom}}(x + e)) \triangleq \mathcal{L}_f h(x) + \mathcal{L}_g h(x)k_{\text{nom}}(x + e), \quad (9)$$
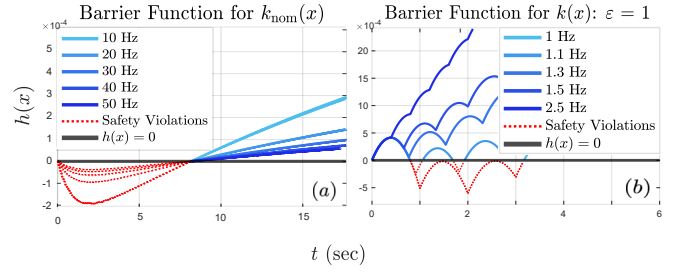

Fig. 1. (a) Safety under the nominal controller via sample-and-hold. Here, violations are encountered regardless of the sampling frequency, thus requiring set expansions to accommodate sampling errors. (b) Robustness of the control adjustment proposed in Section IV. Here, we are guaranteed to satisfy safety at slower sampling frequencies than (a). Both (a) and (b) are initialized from $h(x) = 0$ (i.e., the set boundary) and correspond to the adaptive cruise control system presented in Section V.

which may no longer satisfy the desirable barrier condition:

$$\dot{h}(x, k_{\text{nom}}(x + e)) \geq -\alpha(h(x)). \quad (10)$$

Thus, safety of the sample-and-hold system on $\mathcal{C}$ cannot be guaranteed without an additional assumption accounting for sample-and-hold errors, which is why practical safety considers allowing minor safety violations. Similarly, ISSf establishes that small errors yield minor safety violations if there exists a function ι such that the ISSf-BC holds:

$$\dot{h}(x, k_{\text{nom}}(x + e)) \geq -\alpha(h(x)) - \iota(\|e\|). \quad (11)$$

The following regularity assumptions allow us to obtain (11).

Assumption 1. *(Lipschitz Dynamics):* The functions f, g and the controller k are Lipschitz continuous on $\mathbb{R}^n$. •

Assumption 2. *(Upper Bound on $\mathcal{L}_g h$):* The function $\mathcal{L}_g h$ is bounded above. That is, there exists a positive constant $\lambda > 0$ such that $\|\mathcal{L}_g h(x)\| \leq \lambda$ for all $x \in \mathcal{C}$. •

Remark 1. *(Regularity Assumptions on Region of Operation):* Throughout this paper, we make regularity assumptions on bounds, as well as Lipschitzness, on different functions. We note that these terms are only required along the trajectories. Usually, there are multiple safety constraints (with possible additional stability constraints) in practice. Our bounds do not need to hold for all points in each safe set, but rather in their intersection where system trajectories are feasible, i.e., *region of operation*. To this end, if the final *region of operation* is compact, then all bounds exist, and Lipschitzness only needs to be local. •

Under Assumptions 1-2, we derive the ISSf-BC (11) as:

$$\dot{h}(x, k_{\text{nom}}(x + e)) = \mathcal{L}_f h(x) + \mathcal{L}_g h(x)k_{\text{nom}}(x)$$
$$+ \mathcal{L}_g h(x)\big(k_{\text{nom}}(x(t_i)) - k_{\text{nom}}(x)\big)$$
$$\geq -\alpha(h(x)) - \underbrace{L_k \lambda \|e\|}_{\iota(\|e\|)}, \quad (12)$$

for $x \in \mathcal{C}$, where $L_k > 0$ is the Lipschitz constant of the controller. Typically, the ISSf-BC can be used to establish forward invariance of an expanded set $\mathcal{D} \supset \mathcal{C}$ in the form:

$$\mathcal{D} = \{x \in \mathbb{R}^n : h_d(x) = h(x) + d \geq 0\}, \quad (13)$$

for some positive constant $d > 0$ dictating the size of safety violation being accommodated. However, the bound λ used in (12) only holds on the set $\mathcal{C}$ as stated in Assumption 2. Therefore a new bound $\lambda' > \lambda$ must first be established on $\mathcal{D}$. Note importantly that we may not directly assume a bound λ' on $\mathcal{D}$ because we use it to help define $\mathcal{D}$. To establish the existence of a λ', we make another regularity assumption:

Assumption 3. *(Lipschitz Continuity of $\mathcal{L}_g h$):* The function $\mathcal{L}_g h$ is Lipschitz continuous on $\mathbb{R}^n$. That is, $\exists\ M > 0$ such that $\|\mathcal{L}_g h(x) - \mathcal{L}_g h(y)\| \leq M\|x - y\|\ \forall\ x, y \in \mathbb{R}^n$. ●

The above assumption allows us to characterize the behavior of $\mathcal{L}_g h$ locally in the neighborhood of $\mathcal{C}$. In particular, consider a δ-neighborhood of $\mathcal{C}$, denoted by $\mathcal{S}$. Because $\|x\|_{\mathcal{C}} < \delta$ for all $x \in \mathcal{S}$, we can show that:

$$\begin{aligned}\|\mathcal{L}_g h(x)\| &\leq \|\mathcal{L}_g h(x) - \mathcal{L}_g h(y)\| + \|\mathcal{L}_g h(y)\| \\ &\leq M\|x\|_{\mathcal{C}} + \lambda \\ &\leq M\delta + \lambda = \lambda',\end{aligned}$$

for all $x \in \mathcal{S}$, and the following property holds:

$$\dot{h}(x, k_{\mathrm{nom}}(x + e)) \geq -\alpha(h(x)) - L_k \lambda' \|e\|. \tag{14}$$

This shows that the ISSf-BC holds where safety violation is minor (close to the original safe set $\mathcal{C}$). Nevertheless, we cannot yet establish safety on $\mathcal{D}$ because there is no guarantee that $\mathcal{D}$ will be in the neighborhood of $\mathcal{C}$. For instance, by adjusting the parameter d from zero, the set $\mathcal{D}$ may depart from $\mathcal{C}$ unboundedly to infinity. In such a case, however, it simply means the barrier function h is not a good measure for minor safety violations and is unsuitable for formalizing practical safety. Thus, we make the following assumption.

Assumption 4. *(Proximal Level Curves):* The level curves of h are within a certain distance from its zero level curve $\partial\mathcal{C}$. That is, given a constant $d > 0$ such that $h^{-1}(d)$ is nonempty, there exists an upper bound $\delta > 0$ such that $\|x\|_{\partial\mathcal{C}} < \delta$ for all $x \in h^{-1}(-d)$. ●

The above assumption requires that h is a suitable measure for minor safety violations, as well as practical safety. Indeed, the idea is related to ideas such as upper semi-continuity of level sets [26], [27] and coercivity [3], which can be obtained under mild conditions. We omit those details and simply make the above assumption in the interest of space and to avoid drifting away from the main narrative with mathematical details. The following theorem formalizes the notion of minor safety violations assumed in practical safety:

Theorem 1. *(Forward Invariance of Expanded Set $\mathcal{D}$): Consider the sample-and-hold control system* (8). *Under Assumptions 1-4, for each $d > 0$, there exists an upper bound $e_{\max} > 0$ on the sample-and-hold error such that, if $\|e\|_\infty \leq e_{\max}$, the set $\mathcal{D}$ given in* (13) *is forward invariant.*

Proof. We begin by noting that under Assumption 4, there exists a $\delta > 0$ such that $\lambda' = M\delta + \lambda$ is the upper bound

on $\mathcal{L}_g h$ on set $\mathcal{D}$, and thus, (14) holds. Defining $e_{\max} = -\alpha(-d)/L_k\lambda'$, we have:

$$\begin{aligned}\dot{h_d}(x, k_{\mathrm{nom}}(x + e)) &= \dot{h}(x, k_{\mathrm{nom}}(x + e)) \\ &\geq -\alpha(h(x)) - L_k \lambda' e_{\max} \\ &= -\alpha(h_d(x) - d) + \alpha(-d) = -\alpha_d(h_d(x))\end{aligned}$$

where $\alpha_d(r) = \alpha(r - d) - \alpha(-d)$. Because $\alpha_d(0) = 0$ and α is a class-$\mathcal{K}_\infty^e$, α_d is also a class-$\mathcal{K}_\infty^e$. Thus, the expanded set $\mathcal{D}$ is forward invariant, concluding the proof. □

The theorem above justifies expanding the set $\mathcal{C}$ to accommodate small sample-and-hold errors. Our result is based on the ISSf concept, particularly through the ISSf-BC in (14). We note importantly, however, that our ISSf-BC (14) only holds on $\mathcal{D}$ and cannot accommodate arbitrarily large $\|e\|$ even if we select d to be large, unlike the standard ISSf. This limitation arises because λ' depends on d, and as a result, our function ι in (6) is not uniform for all d. Fortunately, we avoid arbitrarily large sample-and-hold errors through high frequency sampling, which we discuss next.

C. Small Error Bounds

Our next step is to establish a relationship between the error $\|e\|$ and time between two sampling instants. Recall that at each instant t_i, the controller is sampled, and $e(t_i) = 0$ by definition. It follows intuitively that if only a short time elapses before the next sampling instant t_{i+1}, then $\|e\|$ should not grow much. This relies on the following assumption:

Assumption 5. *(Bounded Dynamics):* The dynamics describing sample-and-hold control-affine system (8) are bounded on a given safe set $\mathcal{C}$, i.e. $\|\dot{x}\| = \|f(x) + g(x)k(x + e)\| \leq B_e$ for all $x \in \mathcal{C}$ with a positive constant B_e. ●

Once again, the assumption on boundedness is justified by the fact that it holds for compact safe sets (or compact regions of operation, cf. Remark 1). From a similar argument as $\mathcal{L}_g h$, it follows that under Assumption 1, 4 and 5, there exists a bound $B_e' \geq B_e$ on the set $\mathcal{D}$, providing a sufficient condition for establishing a sample-and-hold error bound.

Lemma 1. *(Bounded Error): Consider the sample-and-hold system* (8). *Let $T_s = t_{i+1} - t_i$ denote the inter-event time between two sampling instants. Under Assumption 1, 4, and 5, the sample-and-hold error is bounded as $\|e(t)\| \leq B_e' T_s$ for all $t \in [t_i, t_{i+1})$ if the states along the trajectory $t \mapsto x(t)$ remain in the expanded set $\mathcal{D}$.*

Proof. From $e(t) = x(t_i) - x(t)$, we have $\dot{e}(t) = -\dot{x}(t)$. Then, by considering the evolution of $\|e(t)\|$, because the state remains in the set $\mathcal{D}$, the following bound holds:

$$\|e(t)\| = \left\| \overbrace{e(t_i)}^{0} + \int_{t_i}^{t} \overbrace{-(f(x(\tau)) + g(x(\tau))k_{\mathrm{nom}}(x(t_i)))}^{\dot{e}(\tau)}\, d\tau \right\|$$

$$\leq \int_{t_i}^{t} B_e'\, d\tau = B_e'(t - t_i).$$

Given the inter-event time $T_s = t_{i+1} - t_i$, we obtain $\|e(t)\| \leq B'_e T_s$ for all time $t \in [t_i, t_{i+1})$, concluding the proof. $\qquad \square$

These constructions enable us to formalize practical safety.

D. Formalizing Practical Safety

We combine Theorem 1 and Lemma 1 to formalize practical safety with the following result:

Theorem 2. *(Practical Safety via ISSf): Consider the sample-and-hold control system* (8) *with periodic sampling instants* $\{t_i\}_{i=0}^{\infty}$, *i.e.,* $t_{i+1} - t_i = T_s$ *for all* $i \in \mathbb{N}$. *Under Assumptions 1-5, for each* $d > 0$, *there exists a sampling time* $T_s > 0$ *small enough such that the expanded set* $\mathcal{D}$ *given in* (13) *is forward invariant.*

Proof. We begin by substituting the error bound from Lemma 1 into the ISSf-BC in (14) to obtain:

$$
\begin{aligned}
\dot{h}_d(x, k_{\text{nom}}(x + e)) &\geq -\alpha(h(x)) - L_k \lambda' \|e\| \\
&\geq -\alpha(h(x)) - L_k \lambda' B'_e T_s \\
&= -\alpha(h_d(x) - d) - L_k \lambda' B'_e T_s \\
&= -\alpha_d(h_d(x)) - \alpha(-d) - L_k \lambda' B'_e T_s
\end{aligned}
$$

where α_d is defined in Theorem 1. From the expression above, we can see that any sampling time satisfying $T_s \leq \frac{-\alpha(-d)}{L_k \lambda' B'_e}$ ensures $\dot{h}_d(x, k_{\text{nom}}(x + e)) \geq -\alpha_d(h_d(x))$, rendering $\mathcal{D}$ forward invariant. This concludes the proof. $\qquad \square$

We have formalized the concept of practical safety within the framework of Input-to-State Safety (ISSf). By leveraging the key assumptions underlying practical safety, we have shown that the safety of sample-and-hold control systems can be established on an expanded set that accommodates the errors by allowing safety violations on the original safe set. However, we explore an alternative strategy in the following section that guarantees safety on the original safe set, avoiding any violations.

IV. VIOLATION-FREE SAMPLE-AND-HOLD SAFETY

This section presents an alternative strategy of achieving safety of the sample-and hold system (8) given a desired sampling time. Formalizing practical safety with the ISSf concept in the previous section provides tools we can leverage to make safety guarantees on the original safe set $\mathcal{C}$. While typically, ISSf involves expanding sets to accommodate errors (i.e., violations of the original set), we explore an alternative approach of guaranteeing safety without resorting to the expansion of the set $\mathcal{C}$. In particular, we make use of the nominal controller k_{nom} and leverage the fact that it satisfies the ISSf-BC (12). Our strategy introduces a robustness term (without expanding the safe set) in the ISSf-BC to deal with the sample-and-hold error. Specifically, we propose the following adjustment of the nominal controller:

$$
k(x) = k_{\text{nom}}(x) + \frac{1}{\varepsilon} \mathcal{L}_g h(x)^\top, \tag{15}
$$

with a tuning parameter $\varepsilon > 0$ to be specified. The term $\frac{1}{\varepsilon} \mathcal{L}_g h(x)^\top$ adjusts a nominal controller in the direction that

increases the barrier function h, which will provide robustness against sample-and-hold errors. However, the newly added term itself will also suffer from errors due to sample-and-hold, and so careful analysis is needed to assess the full benefit of the adjustment.

A. Safety from Controller Adjustment

We begin by first acknowledging that the added term in the controller (15) is only useful when $\mathcal{L}_g h$ is nonzero. Fortunately, we only require this at the boundary of the set.

Assumption 6. *(Control Authority on the Boundary of the Safe Set):* The function $\mathcal{L}_g h$ is bounded from below on the boundary of the safe set $\partial \mathcal{C}$. That is, there exists a positive constant $\mu > 0$ such that $\|\mathcal{L}_g h(x)\| \geq \mu$ for all $x \in \partial \mathcal{C}$. $\quad \bullet$

This assumption is related to the possibility of rendering any safe set forward invariant in the presence of sample-and-hold errors. For states x where $\mathcal{L}_g h(x) = 0$, the barrier function h evolves at the mercy of the drift f, as there is no way of influencing it with any control input. Thus, there is no guarantee that the set will remain forward invariant under sample-and-hold control. In essence, this assumption ensures the well-posedness of the problem we set out to solve. Given the above assumptions and the adjusted controller, we establish the existence of a sampling time that guarantees the safety of (8) on $\mathcal{C}$ in the following result.

Theorem 3. *(Safety on Original Safe Set with Adjusted Controller): Consider the sample-and-hold control system* (8) *using the adjusted controller provided in* (15) *instead of* k_{nom}. *Let the controller be sampled periodically with a sampling time* T_s, *then under the Assumptions 1-3, 5 and 6, there exists a small (fast) enough sampling time* T_s *such that the following condition holds:*

$$
\dot{h}(x, k(x + e)) \geq -\alpha(h(x)), \tag{16}
$$

for states x *on a small* δ-*neighborhood of* $\partial \mathcal{C}$. *Hence, the safe set* $\mathcal{C}$ *is forward invariant.*

Proof. We begin by noting that under Assumptions 3 and 6, there exists a nonzero lower bound $\mu' \leq \mu$ for the function $\|\mathcal{L}_g h\|$, within the δ-neighborhood of the set boundary $\partial \mathcal{C}$. We can establish the following ISSf-BC on $\partial \mathcal{C}$:

$$
\begin{aligned}
&\dot{h}(x, k(x + e)) \\
&= \mathcal{L}_f h(x) + \mathcal{L}_g h(x)\left(k_{\text{nom}}(x_i) + \frac{1}{\varepsilon} \mathcal{L}_g h(x_i)^\top\right) \\
&\geq -\alpha(h(x)) - \|\mathcal{L}_g h(x)\| L_k \|e\| + \frac{1}{\varepsilon} \mathcal{L}_g h(x) \mathcal{L}_g h(x_i)^\top \\
&= -\alpha(h(x)) - \|\mathcal{L}_g h(x)\| L_k \|e\| + \frac{1}{\varepsilon} \|\mathcal{L}_g h(x)\|^2 \\
&\quad + \frac{1}{\varepsilon} \mathcal{L}_g h(x)(\mathcal{L}_g h(x_i) - \mathcal{L}_g h(x))^\top \\
&\geq -\alpha(h(x)) + \|\mathcal{L}_g h(x)\|\left(\frac{1}{\varepsilon} \|\mathcal{L}_g h(x)\| - (L_k + \frac{M}{\varepsilon})\|e\|\right) \\
&\geq -\alpha(h(x)) + \|\mathcal{L}_g h(x)\|\left(\frac{\mu'}{\varepsilon} - (L_k + \frac{M}{\varepsilon})\|e\|\right), \tag{17}
\end{aligned}
$$

where we have used the shorthand notation $x_i = x(t_i)$. Next, similar to the result of Lemma 1, under Assumption 5, we

can establish an error bound $\|e(t)\| \leq BT_s$ where B is the bound on our dynamics (8) with the controller (15), instead of k_{nom}. This leads to the following:

$$\dot{h}(x, k(x + e)) \tag{18}$$
$$\geq -\alpha(h(x)) + \|\mathcal{L}_g h(x)\| \left(\frac{\mu'}{\varepsilon} - (L_k + \frac{M}{\varepsilon}) BT_s \right).$$

By picking $T_s < \mu'/(B(\varepsilon L_k + M))$ to make the last term positive, the barrier condition $\dot{h}(x, k(x + e)) \geq -\alpha(h(x))$ is met on $\partial \mathcal{C}$, i.e., $\dot{h}(x, k(x + e)) \geq 0$ where $h(x) = 0$. In addition, due to Assumption 6, $\frac{\partial h}{\partial x} \neq 0$ on $\partial \mathcal{C}$, so by Nagumo's theorem [25], the set $\mathcal{C}$ is forward invariant. $\quad\square$

The above theorem establishes a violation-free inter-sampling result. The result shows that with an adjustment to the controller, the sample-and-hold system can be rendered safe on the original safe set $\mathcal{C}$, with a high enough sampling frequency. However, this result does not provide any barrier condition (3) for every state x in the safe set $\mathcal{C}$. This may be problematic as many safety-related concepts in the literature may rely on such a condition. One particular example is event-triggered control, which we discuss in Section IV-C.

B. Barrier Condition for Adjusted Controller

In order to derive a barrier condition for the entirety of the safe set $\mathcal{C}$, we note one key obstruction. That is, there is a possibility that $\mathcal{L}_g h$ may approach zero for states at least δ away from the boundary of the safe set, i.e., for $x \in \mathcal{C}$ such that $\|x\|_{\partial \mathcal{C}} > \delta$. In such a case, our adjustment in (15) to the nominal controller is ineffective. Nevertheless, we can use the following fact:

$$\alpha(h(x)) = (1 + c)\alpha(h(x)) - c\alpha(h(x))$$
$$= \alpha'(h(x)) - c\alpha(h(x)), \tag{19}$$

for any positive constant $c > 0$, and the function $\alpha' = (1 + c)\alpha$ is also a class-$\mathcal{K}^e_\infty$ function. The idea is to leverage the fact that $h(x) \neq 0$ inside the safe set, to use $c\alpha(h(x))$ to provide the necessary robustness against the sample-and-hold error. To this end, we make the following assumption.

Assumption 7. *(Lower Bound on h):* For any given $\delta > 0$, there exists $h_{\min} > 0$ such that $h(x) \geq h_{\min}$ for all $x \in \mathcal{C}$ such that $\|x\|_{\partial \mathcal{C}} \geq \delta$. $\quad\bullet$

The assumption is based on the idea that barrier function h should be a proper safety measure, ensuring it has higher values farther away from unsafe states. The property (19) and the controller (15) ultimately lead to a barrier condition for every $x \in \mathcal{C}$, which we present in the following theorem:

Theorem 4. *(Barrier Condition on Original Safe Set with Adjusted Controller): Consider the sample-and-hold control system* (8) *using the adjusted controller provided in* (15) *instead of* k_{nom}. *Let the controller be sampled periodically with a sampling time T_s, under the Assumptions 1-3 and 5-7, there exists a small (fast) enough sampling time T_s such that the following condition holds:*

$$\dot{h}(x, k(x + e)) \geq -\alpha'(h(x)), \tag{20}$$

for all $x \in \mathcal{C}$. Hence, the safe set $\mathcal{C}$ is forward invariant.

Proof. From Theorem 3, we note that:

$$\dot{h}(x, k(x + e)) \geq -\alpha(h(x)) \geq -\alpha'(h(x)),$$

on a small δ-neighborhood under the assumption of the theorem. Therefore, we will focus on states x such that $\|x\|_{\partial \mathcal{C}} \geq \delta$. To this end, Assumption 7 dictates that $h(x) \geq h_{\min}$, so we have $\alpha(h(x)) \geq \alpha(h_{\min})$. Following the proof of Theorem 3, we obtain the following inequality:

$$\dot{h}(x, k(x + e)) \geq -\alpha'(h(x)) + c\alpha(h_{\min}) + \frac{\|\mathcal{L}_g h(x)\|^2}{\varepsilon}$$
$$\quad - \|\mathcal{L}_g h(x)\| \left((L_k + \frac{M}{\varepsilon}) BT_s \right)$$
$$\geq -\alpha'(h(x)) + c\alpha(h_{\min}) - \lambda \left(L_k + \frac{M}{\varepsilon} \right) BT_s.$$

Thus, we establish a safe sampling time by picking a sampling time satisfying:

$$T_s < \min \left\{ \frac{c\alpha(h_{\min})}{\lambda(L_k + \frac{M}{\varepsilon})} \, , \, \frac{\mu'}{B(\varepsilon L_k + M)} \right\}, \tag{21}$$

we ensure that the barrier condition (20) is met for all $x \in \mathcal{C}$, concluding the proof. $\quad\square$

The above theorem establishes a barrier condition for all $x \in \mathcal{C}$ by ensuring that, with the adjusted controller (15), robustness against sample-and-hold errors is always guaranteed for the system (8). In contrast to the strategy of set expansions discussed in Section III-A, Theorem 4 ensures safety on the original set $\mathcal{C}$, avoiding violations.

The main drawback of Theorem 4 is its conservatism in the sampling time it guarantees. In presenting our theorem statement, we elect to omit the bound on the safe sampling time T_s because it involves various constants B, λ, μ', M, L_k, which are difficult to obtain in practice. In addition, our derivations are overly conservative at some key steps. For instance, the bound on sample-and-hold error in Lemma 1 supposes the state deviates as fast as possible from the state where it is last sampled. To resolve this, we leverage the results in this section to propose an event-triggered approach that efficiently samples the controller.

C. Violation-Free Event Triggered Safety

Event-triggered control, as proposed in [19], [24] offers a way to mitigate conservatism in controller sampling. In this framework, the control is sampled at time instants (i.e., events) prescribed by a state-based criterion, rather than periodically based on time. Most importantly, in our context, we can leverage the barrier condition developed in Theorem 4 to establish a trigger condition that ensures the sample-and-hold system (8) is safe on $\mathcal{C}$. To this end, we use the following reasonable trigger condition to maintain safety:

$$\mathcal{T}(x, e) = \dot{h}(x, k(x + e)) + \alpha'(h(x)). \tag{22}$$

The event-triggered idea is to monitor (22) to make sure it always remains positive, that is, $\mathcal{T}(x(t), e(t)) > 0$ along the

trajectory and to trigger a control sampling only when it gets violated as:

$$t_{i+1} = \min \left\{ t \geq t_i : \mathcal{T}(x(t), e(t)) = 0 \right\}. \quad (23)$$

The main concern with event-triggered control is related to its aperiodic nature of controller samplings. More specifically, it becomes possible that an infinite number of controller samplings are triggered within a finite time period (Zeno behavior). Fortunately, the existence of a sampling time provided by Theorem 4 eliminates this possibility. We now formalize our event-triggered control strategy.

Theorem 5. *(Trigger Law for Safety on $\mathcal{C}$): Consider the sample-and-hold system* (8) *with a adjusted controller given by* (15). *Let the sequence of sampling time* $\{t_i\}_{i \in \mathbb{N}}$ *be determined iteratively according to the trigger law* (23). *Under Assumptions 1-3 and 5-7, there exists a minimum inter-event time $T_s > 0$ such that $t_{i+1} - t_i \geq T_s$ for all $i \in \mathbb{N}$. Consequently, the barrier condition* (20) *is satisfied for all time along the trajectory, and the set $\mathcal{C}$ is rendered forward invariant.*

Proof. Under the assumptions, we can follow the proof of Theorem 4 to guarantee the existence a $T_s > 0$ that ensures the quantity $\mathcal{T}(x(t), e(t))$ cannot become negative before T_s has elapsed. It can then be concluded that $t_{i+1} - t_i \geq T_s$ for all $i \in \mathbb{N}$. Combining this with the fact that the trigger condition (23) ensures that $\mathcal{T}(x(t), e(t)) > 0$ ensures that $\dot{h}(x(t), k(x(t) + e(t))) > -\alpha'(h(x(t)))$ along the trajectories, and $\mathcal{C}$ is forward invariant. $\square$

The theorem above establishes an event-triggered strategy that ensures the safety of the sample-and-hold control system (8) on the set $\mathcal{C}$. Moreover, there is no need to specify the various bounds to obtain a suitable sampling time as required in Theorem 4. Instead, to utilize event-triggered control, we note that any positive values of $c > 0$ and $\varepsilon > 0$ are sufficient, albeit small values of these parameters will result in a higher sampling rate while large values will result in lack of robustness or larger control input, respectively. We now illustrate the effectiveness of our violation-free sample-and-hold safety design through simulation experiments.

V. APPLICATION TO ADAPTIVE CRUISE CONTROL

We apply our results to the adaptive cruise control system, where a host vehicle is controlled to follow a lead vehicle while maintaining a safe distance with it's leader. We define $x = (x_1, x_2, x_3)$, where x_1 represents the position of the host vehicle, x_2 represents its velocity, and x_3 represents the headway distance between the host and the lead vehicle. We adopt the following point-wise model for the dynamics [28]:

$$\dot{x} = \begin{bmatrix} x_2 \\ -\frac{1}{m} F_r \\ v_0 - x_2 \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{m} \\ 0 \end{bmatrix} u,$$

where $F_r = f_0 + f_1 x_2 + f_2 x_2^2$ represents the resistance force (in Newtons N) experienced by the host vehicle while m is it's mass. v_0 denotes a constant velocity of the leading
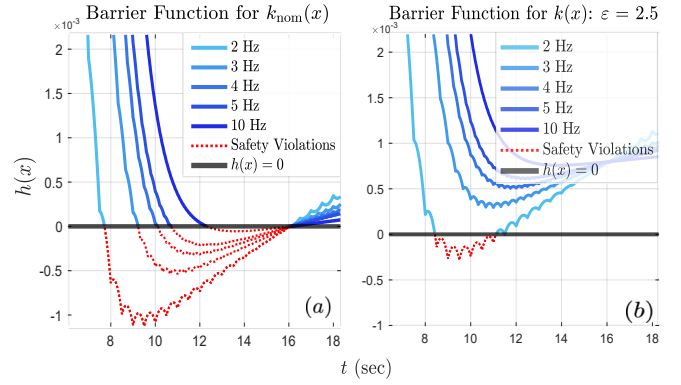

Fig. 2. Illustration of the relationship between sampling frequency and ε and their satisfaction of safety, initialized from a positive value of h.

vehicle. Motivated by [28], we take $m = 1650\,kg, v_0 = 13.89\,\frac{m}{s}, f_0 = 0.1N, f_1 = 5\,\frac{Ns}{m}$ and $f_2 = 0.25\,\frac{Ns^2}{m}$.

A. Nominal Controller

We use a nominal controller to direct the host vehicle towards a desired specified speed $v_d = 22\,\frac{m}{s}$. When the host vehicle enters unsafe regions, a safety controller takes over by minimally adjusting the nominal control input. To implement the desired objective, we employ the desired controller detailed in [28]:

$$u_{des}(x) = -\bar{\varepsilon}\frac{m}{2}(x_2 - v_d) + F_r(x), \quad (24)$$

where $\bar{\varepsilon} = 10$ is presented in [28] as the decay rate necessary for the stability of x_2 to v_d.

B. Safety Controller

In contrast to the approach taken in [28], we adopt a nonlinear model structure for time headway by incorporating a variable time headway [29] in the barrier function:

$$h(x) = x_3 - T_h(x)x_2.$$

Here, $T_h(x) = 1.8x_2$ varies depending on the host vehicle's speed and a constant value of 1.8. By taking the derivative of our barrier function, we obtain:

$$\dot{h}(x, u) = (v_0 - x_2) + \frac{3.6x_2 F_r}{m} - \frac{3.6x_2}{m}u$$

To ensure safety, we implement a Quadratic Program (QP) based safety controller that minimally adjusts u_{des} through a safety filter [14]:

$$k_{nom}(x) = \underset{u \in \mathbb{R}}{\arg\min} \, ||u - u_{des}(x)||^2 \quad \text{(CBF-QP)}$$

$$\text{s.t. } \dot{h}(x, u) \geq -\alpha(h(x)).$$

C. Simulation Results

We adjust $k_{nom}(x)$ from the above CBF-QP with the proposed method (15) and examine its capability of achieving safety in Fig. 2, under various sampling frequencies, with parameters $c = 9.18$, $h_{min} = 0.0005$, and $\varepsilon = 2.5$. It can be seen that slower sampling frequencies result in safety violations. However, by utilizing Theorems 3 and 4, there exists fast enough sampling frequencies that achieve safety
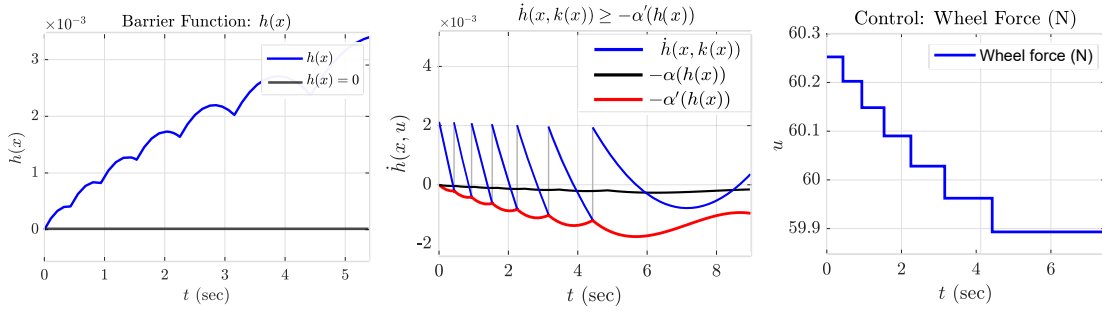
Fig. 3. Event Triggered Control results showing (from left to right): barrier function values, trigger condition satisfaction, and sampled control values.

on the original safe set $\mathcal{C}$. Additionally, we implement the event-triggered control strategy proposed in Theorem 5, and demonstrate its satisfaction of safety on the original safe set (Figs. 3-left and 3-center), with aperiodic event-triggered sampling (Fig. 3-right). Safety is automatic under the event-triggered sampling (Fig. 3-left), unlike the time-triggered strategy that requires a heuristic determination (Fig 1(b)).

VI. CONCLUSION

We have formalized practical safety through the Input-to State Safety framework. From this new perspective, we have proposed an alternative method of achieving sample-and-hold safety without any set violations (i.e., set expansions). Our approach involves adjusting the nominal controller to provide robustness near the boundary of the safe set. Furthermore, our analysis has enabled us to leverage event-triggered control for safety, and thus, we can mitigate the conservatism in choosing a sampling frequency. Future work involves the extension of our work to study the effects of measurement errors associated with the sampling of safeguarding controllers.

REFERENCES

[1] M. Pelgrom, *Analog-to-Digital Conversion*. New York: Springer, 2010.
[2] A. Ayush and S. Koushil, "Discrete control barrier functions for safety-critical control of discrete systems with application to bipedal robot navigation," in *Robotics: Science and Systems*, vol. 13, Cambridge, MA, 2017.
[3] A. J. Taylor, V. D. Dorobantu., R. K. Cosner, Y. Yue, and A. D. Ames, "Safety of sampled-data systems with control barrier functions via approximate discrete time models," in *2022 IEEE 61st Conference on Decision and Control (CDC)*, pp. 7127–7134, 2022.
[4] W. Shaw Cortez, D. Oetomo, C. Manzie, and P. Choong, "Control Barrier Functions for Mechanical Systems: Theory and Application to Robotic Grasping," *IEEE Transactions on Control Systems Technology*, vol. 29, pp. 530–545, Mar. 2021. Conference Name: IEEE Transactions on Control Systems Technology.
[5] A. Ghaffari, I. Abel, D. Ricketts, S. Lerner, and M. Krstić, "Safety verification using barrier certificates with application to double integrator with input saturation and zero-order hold," in *2018 Annual American Control Conference (ACC)*, pp. 4664–4669, IEEE, 2018.
[6] J. Breeden, K. Garg, and D. Panagou, "Control barrier functions in sampled-data systems," *IEEE Control Systems Letters*, vol. 6, 2021.
[7] L. Niu and H. Z. A. Clark, "Safety-critical control synthesis for unknown sampled-data systems via control barrier functions," in *2021 60th IEEE Conference on Decision and Control (CDC)*, pp. 6806–6813, IEEE, 2021.
[8] Y. Zhang, S. Walters, and X. Xu, "Control barrier function meets interval analysis: Safety-critical control with measurement and actuation uncertainties," in *American Control Conference (ACC)*, IEEE, 2022.
[9] S. Kolathaya and A. D. Ames, "Input-to-state safety with control barrier functions," *IEEE Control Systems Letters*, vol. 3, no. 1, pp. 108–113, 2018.
[10] E. D. Sontag, "On the Input-to-State Stability Property," *European Journal of Control*, vol. 1, Nov. 1995.
[11] Z.-P. Jiang and Y. Wang, "Input-to-state stability for discrete-time nonlinear systems," *Automatica*, vol. 37, pp. 857–869, June 2001.
[12] R. Freeman and P. V. Kokotovic, *Robust nonlinear control design: state-space and Lyapunov techniques*. Springer Science & Business Media, 2008.
[13] A. Ames, X. Xu, J. 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, 2017.
[14] A. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *European Control Conference*, pp. 3420–3431, June 2019.
[15] M. Jankovic, "Robust control barrier functions for constrained stabilization of nonlinear systems," *Automatica*, vol. 96, 2018.
[16] A. Alan, A. J. Taylor, C. R. He, G. Orosz, and A. D. Ames, "Safe controller synthesis with tunable input-to-state safe control barrier functions," *IEEE Control Systems Letters*, vol. 6, pp. 908–913, 2022.
[17] R. Cosner, M. Tucker, A. Taylor, K. Li, T. Molnar, W. Ubelacker, A. Alan, G. Orosz, Y. Yue, and A. Ames, "Safety-aware preference-based learning for safety-critical control," in *Learning for Dynamics and Control Conference*, pp. 1020–1033, PMLR, 2022.
[18] A. Alan, A. J. Taylor, C. R. He, A. D. Ames, and G. Orosz, "Control barrier functions and input-to-state safety with application to automated vehicles," *arXiv preprint arXiv:2206.03568*, 2022.
[19] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE Transactions on Automatic Control*, vol. 52, no. 9, pp. 1680–1685, 2007.
[20] W. P. M. H. Heemels, K. H. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," in *IEEE Conf. on Decision and Control*, (Maui, HI), pp. 3270–3285, Dec. 2012.
[21] S. Koga, S. Demir, and M. Krstic, "Event-triggered safe stabilizing boundary control for the Stefan PDE system with actuator dynamics," *arXiv preprint arXiv:2210.01454*, 2022.
[22] W. Xiao, C. Belta, and C. G. Cassandras, "Event-triggered control for safety-critical systems with unknown dynamics," *IEEE Transactions on Automatic Control*, pp. 1–16, 2022.
[23] L. Long and J. Wang, "Safety-critical dynamic event-triggered control of nonlinear systems," *Systems & Control Letters*, vol. 162, 2022.
[24] A. J. Taylor, P. Ong, J. Cortés, and A. Ames, "Safety-critical event triggered control via input-to-state safe barrier functions," *IEEE Control Systems Letters*, vol. 5, no. 3, pp. 749–754, 2021.
[25] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.
[26] J. Aubin and H. Frankowska, *Set-valued analysis*. Springer Science & Business Media, 2009.
[27] R. Konda, A. D. Ames, and S. Coogan, "Characterizing safety: Minimal control barrier functions from scalar comparison systems," *IEEE Control Systems Letters*, vol. 5, no. 2, pp. 523–528, 2021.
[28] A. D. Ames, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs with application to adaptive cruise control," in *IEEE Conf. on Decision and Control*, (Los Angeles,CA), pp. 6271–6278, Dec. 2014.
[29] C. Wu, Z. Xu, Y. Liu, C. Fu, K. Li, and M. Hu, "Spacing policies for adaptive cruise control: A survey," *IEEE Access*, vol. 8, pp. 50149–50162, 2020.