

Safety-Critical Event Triggered Control via Input-to-State Safe Barrier Functions

Andrew J. Taylor*, Pio Ong*, Jorge Cortés, and Aaron D. Ames

Abstract—The efficient utilization of available resources while simultaneously achieving control objectives is a primary motivation in the event-triggered control paradigm. In many modern control applications, one such objective is enforcing the safety of a system. The goal of this paper is to carry out this vision by combining event-triggered and safety-critical control design. We discuss how a direct transcription, in the context of safety, of event-triggered methods for stabilization may result in designs that are not implementable on real hardware due to the lack of a minimum interevent time. We provide an example showing this phenomena and, building on the insight gained, propose an event-triggered control approach via Input-to-State Safe Barrier Functions that achieves safety while ensuring that interevent times are uniformly lower bounded.

Index Terms—Discrete event systems; Sampled-data control; Lyapunov methods

I. INTRODUCTION

BALANCING control objectives such as stability and safety with the efficient use of available resources is critical in many modern control applications including robotics and autonomous driving. Event-triggered control provides a framework that allows the prescription of, in a principled way, when certain resources (such as actuators, sensors, access to a communication network with neighboring agents, or even a human) should be utilized in order to guarantee the satisfaction of said control objectives efficiently, see e.g., [17], [8], [6], [14], [11] and references therein. The robustness properties of the original system enable the opportunistic, rather than continuous, use of the resources without compromising the control objective. In this paper we unify event-triggered control with *Input-to-State Safe Barrier Functions* (ISSf-BF) to ensure a system remains safe while efficiently updating its actuation.

Barrier Functions (BFs) [19], [3] have become increasingly popular as a tool for certifying the safety of a nonlinear control system [2]. The impact on safety guarantees endowed by BFs introduced due to actuation errors was quantified in [9] through the notion of *input-to-state safety* (ISSf) and *Input-to-State Safe Barrier Functions*. As the sample-and-hold implementation of controllers in the event-triggered context introduces errors in the actuation, ISSf provides a natural vehicle for designing trigger laws that guarantee a controller still achieves safety. The unification of event-triggered control

with BFs is not a new idea [12], [20], but is often done with the goal of improving stabilization rather than explicitly enforcing safety. Other event-triggered formulations [18] on output- and state-constrained control have employed Barrier Lyapunov Functions (BLFs), a special instance of BFs where the BF is embedded in the Lyapunov function itself, making safety a direct consequence of stabilization. In contrast, here we employ general BFs, which allows us to decouple safety from stability and results in various added benefits, like simplification of the analysis for other control goals; flexibility in adding, removing, or switching between constraints; and less conservative conditions necessary for ensuring safety. Motivated by the work in [17], we use ISSf-BFs to quantify the impact of sample-and-hold actuation error on safety, and design a trigger law for updating actuation to enforce safety.

One challenge in developing event-triggered control approaches for safety is ensuring that the time between events, or *interevent times*, are lower bounded [6], [13], [4]. Such bounds ensure that the resulting controller and trigger law can be practically implemented on systems that can not actuate infinitely quickly. The notion of *Input-to-State Stability* has been used to prove the existence of these bounds in the context of stabilization [10], [17]. In contrast to the task of stabilization, in the context of safety the dynamics of the system, and thus the error dynamics, are not required to vanish as the quantity dictating the triggering of events vanishes. This can lead to events occurring in rapid succession. Similar behavior has been observed in the context of output-based event-triggered control [7]. To address this problem, we employ a mixed event-triggered mechanism [6], [8] together with the notion of an *input-to-state safe set* to achieve lower bounded interevent times.

The main contribution of this paper is an event-triggered control paradigm for achieving safety of nonlinear control systems with uniformly lower bounded interevent times using ISSf-BFs. Unlike stabilization, utilizing existing tools for safety in an event-triggered context may require additional assumptions or relaxations to yield a design that is implementable on real hardware. To this end, we define the *strong ISSf-BF property*, and demonstrate how an arbitrarily small expansion of the safe set leads to uniformly lower bounded interevent times. To the best of our knowledge, [20] is the only result that considers an event-triggered approach for achieving safety with BFs, but jointly considers it with stabilization and only addresses interevent time bounds corresponding to the latter. Our technical approach is the first to ensure safety and guarantee a minimum interevent time using BFs, and is a first step towards the development of safe controllers that optimize the usage of a system's resources.

*Both authors contributed equally.

A. Taylor is with the Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, CA 91125, USA ajttaylor@caltech.edu. P. Ong and J. Cortés are with the Department of Mechanical and Aerospace Engineering, University of California, San Diego, CA 92093, USA, {piong,cortes}@eng.ucsd.edu. A. Ames is with the Department of Mechanical & Civil Engineering, California Institute of Technology, Pasadena, CA 91125, USA ames@caltech.edu.

This work was partially supported by NSF Award ECCS-1917177.

II. EVENT-TRIGGERED STABILITY

In this section we discuss event-triggered control and review the problem of event-triggered stabilization following [17]. This review will motivate our approach for achieving event-triggered safety presented in Sections IV and V.

Consider the nonlinear control system given by:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}; \mathbf{u}); \quad (1)$$

where $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{u} \in \mathbb{R}^m$, and $\mathbf{f} : \mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}^n$ is locally Lipschitz continuous in both arguments on $\mathbb{R}^n \times \mathbb{R}^m$. We further assume that $\mathbf{f}(\mathbf{0}; \mathbf{u}_0) = \mathbf{0}$ for some $\mathbf{u}_0 \in \mathbb{R}^m$. Under the choice of a Lipschitz continuous state-feedback controller $\mathbf{k} : \mathbb{R}^n \rightarrow \mathbb{R}^m$, with $\mathbf{k}(\mathbf{0}) = \mathbf{u}_0$, the closed-loop system dynamics are given by:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x})); \quad (2)$$

The assumption on local Lipschitz continuity of \mathbf{f} and \mathbf{k} implies that for any initial condition $\mathbf{x}_0 := \mathbf{x}(0) \in \mathbb{R}^n$, there exists a maximum time interval $I(\mathbf{x}_0) = [0; t_{\max})$ such that $\mathbf{x}(t)$ is the unique solution to (2) on $I(\mathbf{x}_0)$. In the case $\mathbf{f}(\cdot; \mathbf{k}(\cdot))$ is forward complete, $t_{\max} = \infty$.

In an event-triggered context, the implementation of the feedback control law \mathbf{k} is done by sampling the state at sequential time instances, $t_0; t_1; t_2; \dots$, and evaluating the controller on the corresponding states $\mathbf{x}(t_0); \mathbf{x}(t_1); \mathbf{x}(t_2); \dots$. Between measurements the control input is held constant:

$$\mathbf{u}(t) = \mathbf{k}(\mathbf{x}(t_i)) \quad \forall t \in [t_i; t_{i+1}); \quad (3)$$

The time instances at which the controller is updated are determined by a state-dependent execution rule or trigger law. We define the measurement error as:

$$\mathbf{e}(t) = \mathbf{x}(t) - \mathbf{x}(t_i) \quad \forall t \in [t_i; t_{i+1}); \quad (4)$$

noting that this in conjunction with (3) implies:

$$\dot{\mathbf{x}}(t) = \mathbf{f}(\mathbf{x}(t); \mathbf{k}(\mathbf{x}(t_i))) \quad \forall t \in [t_i; t_{i+1}); \quad (5)$$

The closed-loop dynamics (5) can alternatively be written as:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e})); \quad (6)$$

where $\mathbf{e} \in \mathbb{R}^n$ is the measurement error.

Event-triggered stabilization relies on the robustness to disturbances of the original dynamics, formalized through Input-to-State Stable Lyapunov Functions (ISS-LF) [16], [15]. *Notation:* Throughout the paper we make use of the following basic definitions. A continuous function $\alpha : [0; a) \rightarrow \mathbb{R}_+$, with $a > 0$, is *class K* ($\infty \in K$) if $\alpha(0) = 0$ and α is strictly monotonically increasing. If $a = \infty$ and $\lim_{r \rightarrow \infty} \alpha(r) = \infty$, then α is *class K_∞* ($\infty \in K_\infty$). A continuous function $\beta : (b; \infty) \rightarrow \mathbb{R}$, with $a; b > 0$, is *extended class K* ($\infty \in K_e$) if $\beta(0) = 0$ and β is strictly monotonically increasing. If $a; b = 1$, $\lim_{r \rightarrow \infty} \beta(r) = 1$, and $\lim_{r \rightarrow \infty} \beta(r) = 1$, then β is *extended class K_∞* ($\infty \in K_{\infty, e}$).

Definition 1 (ISS Lyapunov Function (ISS-LF)). A continuously differentiable function $V : \mathbb{R}^n \rightarrow \mathbb{R}_+$ is an *Input-to-State Stable Lyapunov Function (ISS-LF)* for (6), with respect to measurement errors \mathbf{e} , if there exists $\alpha_1; \alpha_2; \alpha_3 \in K_\infty$ and

$\beta \in K_\infty$ such that for all $\mathbf{x}; \mathbf{e} \in \mathbb{R}^n$:

$$\alpha_1(\|\mathbf{x}\|) \leq V(\mathbf{x}) \leq \alpha_2(\|\mathbf{x}\|); \quad (7a)$$

$$\frac{\partial V}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e})) \leq -\alpha_3(\|\mathbf{x}\|) + \alpha_4(\|\mathbf{e}\|); \quad (7b)$$

As in [17], if we define the trigger law to enforce:

$$\|\mathbf{e}(t)\| \leq \beta(\|\mathbf{x}(t)\|) \quad 0 < \beta < 1; \quad (8)$$

the ISS-LF condition (7b) leads to:

$$\frac{\partial V}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e})) \leq -\beta \alpha_3(\|\mathbf{x}\|); \quad (9)$$

implying asymptotic stability of (6) to $\mathbf{x}^* = \mathbf{0}$. The inequality in (8) can be enforced by defining the trigger law as:

$$t_{i+1} = \min_{t \in [t_i; \infty)} \|\mathbf{e}(t)\| \leq \beta(\|\mathbf{x}(t)\|); \quad (10)$$

As is typical in event-triggered control formulations, it is critical to show that such a trigger law does not lead to the control being updated at arbitrarily close time instances [14], or that the *interevent times* $t_{i+1} - t_i; i \in \mathbb{Z}_{\geq 0}$ are lower bounded by a positive constant $\tau_{\min} > 0$, referred to as the minimum interevent time (MIET). This differs slightly from preventing the stronger notion of Zeno behavior [6], in which the series of interevent times converges (implying the lack of a MIET). The results of [17] ensure that a MIET exists under the trigger (9) under the assumption of Lipschitz continuity on compacts of \mathbf{f} , \mathbf{k} , β , and α .

III. INPUT-TO-STATE SAFETY

In this section we provide background information on Barrier Functions (BFs) and Input-to-State Safe Barrier Functions (ISSf-BFs) that will be used to construct an event-triggered control paradigm that ensures safety.

Consider a set $C \subseteq \mathbb{R}^n$ defined as the 0-superlevel set of a continuously differentiable function $h : \mathbb{R}^n \rightarrow \mathbb{R}$, yielding:

$$C = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) \geq 0\}; \quad (11a)$$

$$\partial C = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) = 0\}; \quad (11b)$$

$$\text{Int}(C) = \{\mathbf{x} \in \mathbb{R}^n : h(\mathbf{x}) > 0\}; \quad (11c)$$

We assume that C is nonempty and has no isolated points, that is, $\text{Int}(C) \neq \emptyset$; and $\overline{\text{Int}(C)} = C$. We refer to C as the *safe set*. This construction motivates the following definitions:

Definition 2 (Forward Invariant & Safety). A set C is *forward invariant* if for every $\mathbf{x}_0 \in C$, the solution $\mathbf{x}(t)$ to (2) satisfies $\mathbf{x}(t) \in C$ for all $t \in I(\mathbf{x}_0)$. The system (2) is *safe* on C if the set is forward invariant.

Verifying that the system (2) is safe on a set C can be done via a Barrier Function:

Definition 3 (Barrier Function (BF)). A continuously differentiable function $h : \mathbb{R}^n \rightarrow \mathbb{R}$ is a *Barrier Function (BF)* for (2) on a set $C \subseteq \mathbb{R}^n$ defined as in (11a)-(11c), if there exists $\alpha_1; \alpha_2; \alpha_3 \in K_\infty$ such that for all $\mathbf{x} \in \mathbb{R}^n$:

$$\frac{\partial h}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x})) \leq -\alpha_1(h(\mathbf{x})); \quad (12)$$

As shown in [19], the existence of a barrier function for (2) on a set C is sufficient to prove the safety and asymptotic

stability of \mathcal{C} . To consider the impact of measurement errors on safety, we consider the notion of input-to-state safety [9].

Definition 4 (Input-to-State Safety (ISSf)). Let the signal $\mathbf{e} : \mathbb{R}_+ \rightarrow \mathbb{R}^n$ be essentially bounded and define $ke k_1 = \text{ess sup}_{t \geq 0} ke(t)k_2$. The closed-loop system (6) is *input-to-state safe (ISSf)* on \mathcal{C} with respect to measurement errors \mathbf{e} if there exists $\geq K_1$ and a set $\mathcal{C}_e \subset \mathcal{C}$ defined as:

$$\mathcal{C}_e, \quad \forall \mathbf{x} \in \mathcal{R}^n : h(\mathbf{x}) + (ke k_1) \geq 0; \quad (13a)$$

$$\partial \mathcal{C}_e, \quad \forall \mathbf{x} \in \mathcal{R}^n : h(\mathbf{x}) + (ke k_1) = 0; \quad (13b)$$

$$\text{Int}(\mathcal{C}_e), \quad \forall \mathbf{x} \in \mathcal{R}^n : h(\mathbf{x}) + (ke k_1) > 0; \quad (13c)$$

such that (6) is safe on \mathcal{C}_e .

We refer to \mathcal{C} as an *input-to-state safe set (ISSf set)* if such a set \mathcal{C}_e exists. This definition implies that though the set \mathcal{C} may not be safe, a larger set \mathcal{C}_e , depending on \mathbf{e} , is safe. If $\mathbf{e} = \mathbf{0}$, we recover that the set \mathcal{C} is safe. This motivates the following definition of Input-to-State Safe Barrier Functions:

Definition 5 (Input-to-State Safe Barrier Function (ISSf-BF)). A continuously differentiable function $h : \mathbb{R}^n \rightarrow \mathbb{R}$ is an *Input-to-State Safe Barrier Function (ISSf-BF)* for (6) on a set $\mathcal{C} \subset \mathbb{R}^n$ defined as in (11a)-(11c), if there exists $\geq K_1, \epsilon$ and $\geq K_1$ such that for all $\mathbf{x}; \mathbf{e} \in \mathbb{R}^n$:

$$\frac{\partial h}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e})) - (h(\mathbf{x})) - (ke k_2); \quad (14)$$

As shown in [9], the existence of an ISSf-BF for (6) on \mathcal{C} implies \mathcal{C} is an ISSf set, implying safety and asymptotic stability to the set \mathcal{C}_e .

IV. TOWARDS RESOURCE-AWARE SAFETY: FROM LYAPUNOV TO BARRIERS

To more efficiently utilize actuation resources when implementing safe controllers, we seek to unify the preceding concepts of event-triggered control and input-to-state safety. In this section we discuss challenges that arise in directly transferring ideas from event-triggered stabilization to safety. Given the similarity of the ISS-LF constraint (7b) and the ISSf-BF constraint (14), it is natural to propose a trigger law that enforces:

$$(ke(t)k_2) - (h(\mathbf{x}(t))) \geq 0; \quad (15)$$

implying:

$$\frac{\partial h}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e})) - (1 + \epsilon) (h(\mathbf{x})); \quad (16)$$

This can be interpreted as allowing the system to more quickly approach the boundary of the safe set at the expense of actuation resources. It is important to note that, inside \mathcal{C} , it is possible to satisfy (15) and thus enforce safety, but the inequality is impossible to satisfy outside \mathcal{C} as $(h(\mathbf{x})) < 0$ if $\mathbf{x} \notin \mathcal{C}$. This type of behavior does not arise in the context of event-triggered stabilization, where convergence is to a point. One way to solve this issue is to instead define the trigger law:

$$(ke(t)k_2) - j (h(\mathbf{x}(t))) \geq 0 < j < 1; \quad (17)$$

which enforces (16) if $\mathbf{x} \in \mathcal{C}$ and enforces:

$$\frac{\partial h}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e})) - (1 - \epsilon) (h(\mathbf{x})); \quad (18)$$

if $\mathbf{x} \notin \mathcal{C}$. In this formulation, the system is not only allowed to more quickly approach the boundary, but is also not required to converge to the set as quickly when outside of the set. This is a generalization of event-triggered stabilization to a set.

Even with this solution, it is not guaranteed that this trigger law will have a MIET. Although ruling out Zeno behavior is not required to guarantee safety, unlike stabilization, it is important to have a MIET in term of implementation of the controller (cf. [6]). The key difference between stability and safety leading to the failure of a MIET to exist for a safe event-triggered controller lies in how the system dynamics must behave close to an equilibrium point compared to how they can behave close to the boundary of the safe set. In stabilization, continuity of the dynamics requires the dynamics to vanish as the equilibrium is approached, leading to the error dynamics in (5) vanishing. In safety, the dynamics close to the boundary of the safe set need not vanish as the boundary is approached, such that the error dynamics in (5) need not vanish. We provide the following example to illustrate how this difference can lead to a MIET failing to exist for the trigger design (17).

A. Example

Consider the following system:

$$\frac{d}{dt} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} + \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} u; \quad (19)$$

for which we wish to ensure the safety of the set \mathcal{C} , given by the 0-superlevel set of the continuously differentiable function $h(\mathbf{x}) = 1 - x_1^2 - x_2^2 = 1 - \mathbf{k}\mathbf{x}\mathbf{k}_2^2$. The time derivative of this function along solutions to (19) is given by $h(\mathbf{x}; u) = 2(x_1^2 + x_2^2)u$, for which the state-feedback controller $k(\mathbf{x}) = \frac{1}{2}(1 - x_1^2 - x_2^2)$ yields $h(\mathbf{x}) = (x_1^2 + x_2^2)h(\mathbf{x}) - h(\mathbf{x})$, which implies h is a valid BF for the set \mathcal{C} .

In an event triggered context, the closed-loop dynamics of the system are then given by:

$$\dot{\mathbf{x}}(t) = \begin{bmatrix} k(\mathbf{x}(t_i)) & 1 \\ 1 & k(\mathbf{x}(t_i)) \end{bmatrix} \mathbf{x}(t); \quad (20)$$

for each time $t \geq [t_i; t_{i+1})$. This leads to the time derivative of h along solutions to (20) being given by:

$$h(\mathbf{x}(t); \mathbf{e}(t)) = \mathbf{k}\mathbf{x}(t)\mathbf{k}_2^2 h(\mathbf{x}(t_i)) = \mathbf{k}\mathbf{x}(t)\mathbf{k}_2^2 h(\mathbf{x}(t) + \mathbf{e}(t))$$

for each time $t \geq [t_i; t_{i+1})$, where $\mathbf{e}(t) = \mathbf{x}(t_i) - \mathbf{x}(t)$. To see that the BF h is in fact an ISSf-BF, we note its time derivative can be bounded as follows (we omit the time dependence):

$$\begin{aligned} h(\mathbf{x}; \mathbf{e}) &= \mathbf{k}\mathbf{x}\mathbf{k}_2^2 h(\mathbf{x} + \mathbf{e}) \\ &= \mathbf{k}\mathbf{x}\mathbf{k}_2^2 (1 - \mathbf{k}\mathbf{x}\mathbf{k}_2^2 - 2\mathbf{x}^T \mathbf{e} - \mathbf{e}\mathbf{e}\mathbf{k}_2^2) \\ &= \mathbf{k}\mathbf{x}\mathbf{k}_2^2 (1 - \mathbf{k}\mathbf{x}\mathbf{k}_2^2) - 2\mathbf{k}\mathbf{x}\mathbf{k}_2^3 \mathbf{e}\mathbf{k}_2 \\ &= (1 - \mathbf{k}\mathbf{x}\mathbf{k}_2^2) - 2\mathbf{k}\mathbf{x}\mathbf{k}_2^3 \mathbf{e}\mathbf{k}_2 \\ &= h(\mathbf{x}) - 2r^3 \mathbf{e}\mathbf{k}_2; \end{aligned}$$

for $\mathbf{k}\mathbf{x}\mathbf{k}_2 \leq r$. Given that h is an ISSf-BF on some domain containing the unit circle (choose $r > 1$), the trigger law

enforcing (17) is given by:

$$t_{i+1} = \min t \quad t_i \leq t \leq t_{i+1} \quad \dot{h}(\mathbf{x}(t)) \leq -\alpha h(\mathbf{x}(t)) \quad (21)$$

with $0 < \alpha < 1$. This will guarantee that C is safe as:

$$h(\mathbf{x}; \mathbf{e}) \leq (1 + \alpha) h(\mathbf{x}); \quad \|\mathbf{x}\|_{k_2} \leq 1; \\ (1 - \alpha) h(\mathbf{x}); \quad 1 < \|\mathbf{x}\|_{k_2} < r;$$

Despite f , k , g , and h being Lipschitz continuous on compacts as sufficient in the case of stabilization, the following results shows the trigger design lacks a MIET.

Lemma 1 (MIET does not exist). *The system (20) with the trigger law defined as in (21) does not possess a MIET.*

Proof: To show that the interevent times $t_{i+1} - t_i, i \geq N$ are not lower bounded, we will proceed via contradiction. In particular, let us assume that there exists $\delta > 0$ such that $t_{i+1} - t_i \geq \delta$ for all $i \geq N$. If the state $\mathbf{x}_i = \mathbf{x}(t_i)$ at event time t_i is used as an initial condition, the solution to (20) is:

$$\mathbf{x}(t) = \exp\left(\frac{h(\mathbf{x}_i) - t_i}{2} \begin{bmatrix} \cos t_i & \sin t_i \\ \sin t_i & \cos t_i \end{bmatrix}\right) \mathbf{x}_i; \\ = \mathbf{M}_i(t_i) \mathbf{x}_i;$$

for $t \in [t_i, t_{i+1})$ with $t_i = t - t_i$. Denoting $\delta_i = h(\mathbf{x}_i) - t_i$, we see that the norm of the error is lower bounded by a function monotonically increasing in time:

$$\|\mathbf{e}(t)\|_{k_2} = \frac{\|\mathbf{I} - \mathbf{M}_i(t_i)\|_{k_2} \|\mathbf{x}_i\|_{k_2}}{\exp(\delta_i/2)} \\ = \frac{\|\mathbf{I} - \exp\left(\frac{\delta_i}{2} \begin{bmatrix} \cos t_i & \sin t_i \\ \sin t_i & \cos t_i \end{bmatrix}\right)\|_{k_2} \|\mathbf{x}_i\|_{k_2}}{\exp(\delta_i/2)} \\ = \frac{\|\mathbf{I} - \exp\left(\frac{\delta_i}{2} \begin{bmatrix} \cos t_i & \sin t_i \\ \sin t_i & \cos t_i \end{bmatrix}\right)\|_{k_2} \|\mathbf{x}_i\|_{k_2}}{\exp(\delta_i/2)}$$

This lower bound on the error grows unbounded in time. This implies that no matter the state in $\text{Int}(C)$ that an event occurs, another event must occur at some time in the future (or the bound in (21) will be violated as h is upper bounded on C). Thus, for all $T > 0$, there exists an event time $t_i > T$.

Next, we show that $\lim_{t \rightarrow \infty} h(\mathbf{x}(t)) = 0$. Note that:

$$\dot{h}(\mathbf{x}(t)) = -\alpha h(\mathbf{x}(t)) \quad \|\mathbf{x}(t)\|_{k_2} \leq 1 \quad \exp(h(\mathbf{x}_i) - t_i) \|\mathbf{x}_i\|_{k_2}^2;$$

with time derivative:

$$\dot{h}(\mathbf{x}(t)) = -\alpha h(\mathbf{x}_i) \exp(h(\mathbf{x}_i) - t_i) \|\mathbf{x}_i\|_{k_2}^2;$$

for $t \in [t_i, t_{i+1})$. Within the safe set we have that $h(\mathbf{x}(t)) \geq 0$, such that $h(\mathbf{x}(t))$ is monotonically decreasing in time. The safety of C implies $h(\mathbf{x}(t))$ is lower bounded by 0, and thus we can conclude that $\lim_{t \rightarrow \infty} h(\mathbf{x}(t))$ exists. Assume that this limit is some value $0 < c < 1$. Thus for any $\epsilon > 0$, there exists $T > 0$ such that for $t > T$, $h(\mathbf{x}(t)) < c + \epsilon$. Since there are an infinite number of events, we deduce there exists $t_i > T$ such that $h(\mathbf{x}(t_i)) < c + \epsilon$. As $h(\mathbf{x}(t))$ is monotonically decreasing, it also follows $h(\mathbf{x}(t)) < c$ for all t . This implies:

$$\dot{h}(\mathbf{x}(t)) \leq -\alpha c \exp(c - t_i) (1 - (c + \epsilon)) \leq -\alpha c + \alpha c^2 + \alpha c \epsilon < 0;$$

for $t \in [t_i, t_{i+1})$ where ϵ is chosen small enough to enforce the strict inequality with 0. Thus between two events we have:

$$h(\mathbf{x}(t_{i+1})) \leq h(\mathbf{x}(t_i)) + (-\alpha c + \alpha c^2 + \alpha c \epsilon) \delta;$$

where δ is the assumed MIET. Choosing $\epsilon < (c - c^2)/(1 + c)$ implies $h(\mathbf{x}(t_{i+1})) < c$, contradicting the assumption that $c \leq 0$ (and maintaining the assumption on the existence of δ).

To complete the proof, note $\mathbf{e}(t_i) = \mathbf{0}$ and take the second-order (one-sided) Taylor expansion of $\|\mathbf{e}(t)\|_{k_2}^2$ at $t = t_i$:

$$\|\mathbf{e}(t)\|_{k_2}^2 = \mathbf{e}(t_i)^T \mathbf{e}(t_i) + (t - t_i)^2 + O((t - t_i)^3) \\ = (1 + k(\mathbf{x}(t_i))) k(\mathbf{x}(t_i)) k_2^2 (t - t_i)^2 + O((t - t_i)^3) \\ = k(\mathbf{x}(t_i)) k_2^2 (t - t_i)^2 + c_3 (t - t_i)^3;$$

with $c_3 > 0$. The first term in the inequality follows from $k(\mathbf{x}(t_i)) \geq 0$ for $\mathbf{x}(t_i) \in C$. The second term follows if we view $\frac{d^3}{dt^3} \|\mathbf{e}(t)\|_{k_2}^2$ as a continuous function of the state, which remains within the compact set C . Then $\frac{d^3}{dt^3} \|\mathbf{e}(t)\|_{k_2}^2$ will be bounded for all time as C is forward invariant. This bound in conjunction with Lagrange's Remainder Formula [1] implies the existence of c_3 .

At trigger time t_i , let $h(\mathbf{x}(t_i)) = \delta_i$ with $\delta_i > 0$ arbitrarily small due to the existence of infinite triggers and convergence of h . This implies $k(\mathbf{x}(t_i)) k_2^2 = 1 - \delta_i$. Let $n \in \mathbb{N}$ be such that $\frac{1}{c_3} < n$ and define $t_i^? = t_i + \frac{1}{n} \frac{1 - \delta_i}{c_3}$, noting $t_i^? < t_{i+1}$. It follows from the Taylor expansion that:

$$\|\mathbf{e}(t_i^?)\|_{k_2}^2 \leq \frac{(1 - \delta_i)^3}{c_3^2} \frac{n}{n^3} = \frac{1 - \delta_i}{n^2};$$

As δ_i can be chosen arbitrarily small, we choose it such that:

$$(1 - \delta_i)^3 \leq \frac{2n^3}{4r^6(n-1)^2} \frac{2}{n^2};$$

which indicates that:

$$2r^3 \|\mathbf{e}(t_i^?)\|_{k_2} \leq \|j h(\mathbf{x}(t_i))\| \leq \|j h(\mathbf{x}(t_i^?))\|;$$

as $h(\mathbf{x}(t))$ is monotonically decreasing. As $t_i^? < t_{i+1}$, this contradicts that δ is the MIET. Figure 1 shows the number of events as a function of time and distance from the barrier. The blue curves in Figure 2 correspond to the interevent times. ■

In the proof of Lemma 1 we see the fact that the state dynamics (20) are not required to converge to $\mathbf{0}$ at the boundary of the safe set C leads to the derivative of the measurement error, $\frac{d}{dt} \|\mathbf{e}(t)\|_{k_2}$, being uniformly lower bounded at event

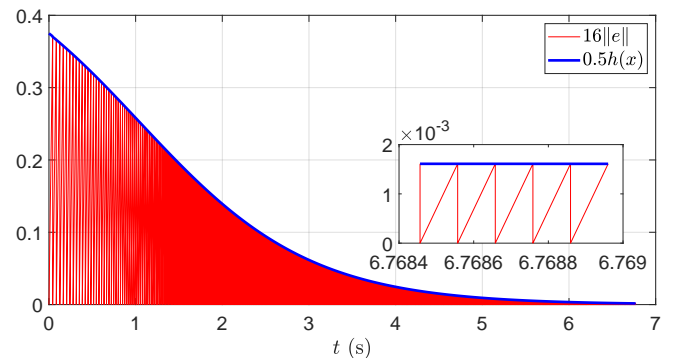


Fig. 1. Simulation results for the system (20) using the trigger law (21). Even as the boundary of the safe set is approached $h(t) \rightarrow 0$, the growth rate of the error does not diminish, leading to arbitrarily small interevent times.

times t_j , which, together with the convergence of h to 0, cf. Figure 1, leads in turn to arbitrarily small interevent times. In particular, the dynamics evolve tangentially to the boundary of the safe set, leading to growing measurement error while moving arbitrarily close to the 0-level set of h .

As the original controller may have additional objectives beyond safety (such as stabilization), it is desirable that the event-triggered implementation not completely eliminate tangential motion near the boundary that may be necessary to achieve the other objectives. To accommodate this, we will introduce a trigger law that limits dynamic evolution tangential to the boundary of the safe set.

V. EVENT-TRIGGERED SAFETY

In this section, we propose an alternative trigger to the one formulated in Section IV that ensures a MIET exists. To resolve the issues highlighted in the preceding example, we introduce the following definition:

Definition 6 (*Strong ISSf Barrier Property*). An ISSf-BF h satisfies the *strong ISSf barrier property* if there exists $d \geq \mathbb{R}$ with $d > 0$ such that for all $\mathbf{x}; \mathbf{e} \in \mathbb{R}^n$:

$$\frac{\partial h}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e})) \leq (h(\mathbf{x})) + d \quad (ke k_2); \quad (22)$$

This property introduces a positive constant, d , into the ISSf-BF condition (14). In the presence of zero measurement error, this enforces that the state dynamics must lie in the interior of the tangent cone [5] when on the boundary of the safe set \mathcal{C} . It also enforces that $\frac{d}{dt}j h(\mathbf{x}(t_j))j$ will be greater than a positive constant as we approach the boundary, similarly to $\frac{d}{dt}ke(t_j)k_2^2$. We now show this property is sufficient to design a trigger law that ensures safety with a MIET.

Theorem 1 (Trigger Law for Safety Critical Systems). *Let h be an ISSf-BF for (6) on a set $\mathcal{C} \subseteq \mathbb{R}^n$ defined as in (11a)-(11c), with corresponding functions $\beta \in \mathcal{K}_{1,e}$ and $\gamma \in \mathcal{K}_1$. Let $\alpha \in \mathcal{K}_{1,e}$, $\delta \in (0; 1]$. If the following assumptions hold:*

- 1) h satisfies the strong ISSf barrier property for a constant $d \in \mathbb{R}$, $d > 0$,
- 2) β is Lipschitz continuous with Lipschitz constant L ,
- 3) there exists $F \in \mathbb{R}$, $F > 0$, such that for all $\mathbf{x}; \mathbf{e} \in \mathbb{R}^n$:

$$\mathbf{k}\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e}))k_2 \leq F;$$

- 4) $\alpha(r) \leq \beta(r)$ for all $r \in \mathbb{R}$,

then the trigger law:

$$t_{i+1} = \min t \geq t_i \mid (ke(t)k_2) = (h(\mathbf{x}(t))) + d; \quad (23)$$

deployed recursively enforces:

$$h(\mathbf{x}; \mathbf{e}) = \frac{\partial h}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e})) \leq (h(\mathbf{x})); \quad (24)$$

thus rendering the set \mathcal{C} safe and asymptotically stable. Furthermore, there exists a MIET given by:

$$t_{i+1} - t_i \geq \frac{d}{LF}; \quad i \in \mathbb{N};$$

Before proving the result, we make a few observations regarding its assumptions. Assumption 3 on the boundedness

of the dynamics need not hold over the entire state space for safety, but can hold for $(\mathbf{x}; \mathbf{e}) \in \mathcal{C} \subseteq \mathbb{R}^n$. Furthermore, if \mathcal{C} is compact, the trigger law enforces the existence of a compact set $E \subseteq \mathbb{R}^n$ such that $\mathbf{e} \in E$. Thus, the continuity of \mathbf{f} and \mathbf{k} implies the assumption is satisfied on $\mathcal{C} \times E$, which also would be sufficient for the result to hold. Assumption 4 ensures the right-hand side of the equality in the trigger will always be positive. β can be viewed as a tuning function which can raise interevent times (but not the MIET) at the expense of less "braking" within the safe set and convergence outside of the safe set. One choice is $\beta(r) = \alpha(r)$, in which case interevent times are lowered for more braking and faster convergence. We note this trigger law can be used in conjunction with (10) to jointly achieve event-triggered stabilization and safety.

Proof: To see the set \mathcal{C} is rendered safe, observe that:

$$\begin{aligned} h &= \frac{\partial h}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e})) \leq (h(\mathbf{x})) + d \quad (ke k_2) \\ &\leq (h(\mathbf{x})) + d \quad (\beta(h(\mathbf{x})) - (h(\mathbf{x})) + d); \\ &= (h(\mathbf{x})) + (1 - \delta)d \quad (h(\mathbf{x})); \end{aligned}$$

implying the barrier condition (12) is satisfied and \mathcal{C} is safe.

To see the interevent time is lower bounded, observe that

$$\begin{aligned} ke(t)k_2 &= e(0) + \int_{t_i}^t (\mathbf{f}(\mathbf{x}(\tau); \mathbf{e}(\tau)))d\tau \\ &= \int_{t_i}^t (\mathbf{f}(\mathbf{x}(\tau); \mathbf{e}(\tau)))d\tau \leq \int_{t_i}^t F d\tau; \end{aligned}$$

This inequality together with the trigger law (23) yields:

$$\begin{aligned} t_{i+1} - t_i &\geq \min t \geq t_i \mid \int_{t_i}^t (\mathbf{f}(\mathbf{x}(\tau); \mathbf{e}(\tau)))d\tau = dg; \\ &\geq \min t \geq t_i \mid \int_{t_i}^t F d\tau = dg = \frac{d}{LF} + t_i; \end{aligned}$$

ensuring the desired result. This in conjunction with the barrier function condition implies \mathcal{C} is asymptotically stable. ■

In the case that an ISSf-BF h does not satisfy the strong barrier property, an auxiliary ISSf-BF, h_b , satisfying the strong ISSf barrier property can be synthesized via h at the expense of guaranteeing only a larger set is kept safe:

Theorem 2 (Strong ISSf Barrier Property in Supersets). *Let h be an ISSf-BF for (6) on a set $\mathcal{C} \subseteq \mathbb{R}^n$ defined as in (11a)-(11c), with corresponding functions $\beta \in \mathcal{K}_{1,e}$ and $\gamma \in \mathcal{K}_1$. Then the function h_b defined as $h_b(\mathbf{x}) = h(\mathbf{x}) + b$, with $b \in \mathbb{R}$, $b > 0$, is an ISSf-BF satisfying the strong ISSf barrier property on the set \mathcal{C}_b defined as:*

$$\mathcal{C}_b = \{ \mathbf{x} \in \mathbb{R}^n \mid h_b(\mathbf{x}) \geq 0 \}; \quad (25)$$

Proof: Observe that:

$$\begin{aligned} \frac{\partial h_b}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e})) &= \frac{\partial h}{\partial \mathbf{x}}(\mathbf{x})\mathbf{f}(\mathbf{x}; \mathbf{k}(\mathbf{x} + \mathbf{e})) \\ &\leq (h(\mathbf{x})) + (ke k_2) \leq (h_b(\mathbf{x}) - b) + (b) \\ &\leq (h_b(\mathbf{x})) + (ke k_2) = \beta_b(h_b(\mathbf{x})) + d_b \quad (ke k_2); \end{aligned}$$

where $\beta_b \in \mathcal{K}_{1,e}$ is defined as $\beta_b(r) = (r - b) + (b)$ and $d_b = (b) > 0$. ■

Thus an ISSf-BF can be used with the trigger law (23) by

