2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Intermittent Safety Filters for Event-Triggered Safety Maneuvers with Application to Satellite Orbit Transfers

Pio Ong and Aaron D. Ames

***Abstract*— In balancing safety with the nominal control objectives, e.g., stabilization, it is desirable to reduce the time period when safety filters are in effect. Inspired by traditional spacecraft maneuvers, and with the ultimate goal of reducing the duration when safety is of concern, this paper proposes an event-triggered control framework with switching state-based triggers. Our first trigger in the scheme monitors safety constraints encoded by barrier functions, and thereby ensures safety without the need to alter the nominal controller—and when the boundary of the safety constraint is approached, the controller drives the system to the region where control actions are not needed. The second trigger condition determines if the safety constraint has improved enough for the success of the first trigger. We begin by motivating this framework for impulsive control systems, e.g., a satellite orbiting an asteroid. We then expand the approach to a more general nonlinear system through the use of safety-filtered controllers. Simulation results demonstrating satellite orbital maneuvers illustrate the utility of the proposed event-triggered framework.**

I. Introduction

The idea of filtering a nominal control action to satisfy safety constraints—that is *safety filtering* [1], [2]—has proven to be a powerful tool in controller synthesis. This technique facilitates the controller design process as we can decouple different control objectives, e.g., stability and safety. An unfortunate consequence of applying safety filters is the possibility that the deviation from the nominal controller will affect the success of the nominal objective, e.g., stability. Addressing this potential conflict involves bounding the deviation from, and the effect on, the nominal controller—a difficult task in nonlinear system.

This paper presents a new approach to safety filtering that is *intermittent* in nature, with the result being event-triggered safety maneuvers. To this end, we take inspiration from safety maintenance of a satellite via orbit transfers [3]. Satellites spend most of their time during a given mission with the nominal objectives, and only apply corrective maneuvers intermittently to ensure safety, e.g., in response to unmodelled environmental dynamics. Because there are periods where no deviation from the nominal controller is needed, guarantees can be made if enough time is spent in these safe operating regions. The goal of this paper is to develop an event-triggered framework that imitates the behavior of satellites that has proven useful in practice. In particular, the switching between safety objective in an "on demand" fashion, and the application of safety filters in an intermittent fashion. The end result will be the introduction of *event-triggered intermittent safety filtering*. The hope is that this will lay the necessary groundwork for an alternative approach enforcing safety guarantees while minimally modifying the nominal performance objectives.

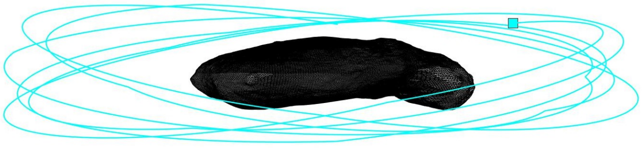

Fig. 1. Satellite safe orbit trajectory around 25143 Itokawa utilizing event-triggered safety maneuvers.

Literature Review

Our paper relies on two main bodies of literature: safety-critical control via certificates, e.g., control barrier functions, and event-triggered control.

Safety-critical controls aims to provide a framework for formally guaranteeing the safety of nonlinear control systems—with safety typically framed as avoiding undesirable states, or equivalently always staying in a set of desirable states. Barrier certificate [4] describes a safety of a set utilizing a scalar function, wherein it is simpler to analyze corresponding violations. In this context, barrier certificates are related to ideas underlying nonovershooting control that restricts outputs [5] or Lyapunov function evolving within a specified bound [6]. Nevertheless, the attractiveness of barrier certificate is that it isolates safety problem from the design of the controller for other objectives, thereby transforming the problem into a more tractable form.

Control barrier functions as first introduced [7] mirror control Lyapunov functions by studying barrier certificates associated with control systems. Yet the result was overly conservative, and as a result the modern form of control barrier functions (CBFs) where introduced in [8]–[11]; these are necessary and sufficient for forward set invariance thereby generalizing Nagumo theorem [12] to control systems. The non-conservative nature of CBFs lead to the idea of a safety filter [1]—and optimization-based controller that minimally modifies a nominal controller to ensure safety. This paper seeks to expand the notion of a safety filter by shortening the filtering period, thereby allowing the nominal controller more freedom. The idea is made possible by event-trigger control.

This research is supported in part by the National Science Foundation (CPS Award #1932091) and Raytheon.

Pio Ong and Aaron D. Ames are with the Department of Mechanical and Civil Engineering, California Institute of Technology, Pasadena, CA 91125, USA. {pioong,ames}@caltech.edu

979-8-3503-0123-6/23/$31.00 ©2023 IEEE

Event-triggered control [13]–[15] synthesizes property preserving discrete implementations of continuous controllers. The seminal work [13] studies sample-and-hold system and proposes an aperiodic sampling scheme that is based on system states rather than fixed time. Event-triggered control shows great improvement in the average sampling time. Event-triggered control implemented in the context of sample-and-hold can be formalized as an impulsive system [16], and in general as a hybrid system [17], [18]. This hints at the possibility of transferring the trigger ideas and applying them to different type of hybrid systems.

In this paper, we study event-triggered control of impulsive systems in the context of safety; this can, for example, be used to describe satellite systems. There are works on event-triggered impulsive control, but they focus on stabilization [19]–[22] which is not applicable to safety because of difference in two objectives, cf. [23]. Additionally, there are works that deal with safety [23]–[25] but not for impulsive control systems. Finally, this paper also studies event-triggered control in the context of intermittent control. Our previous work [26] also considers intermittent control, but in the context of sample-and-hold whereas this paper considers the frequency of safety filtering.

Statement of Contribution

This paper investigates the idea of lengthening the time period during which a safety-critical controller does not need to actively spend control effort in order to satisfy safety constraints. To this end, we use event-triggered control with barrier functions to monitor safety and opportunistically determine when to start applying control for the purpose of satisfying safety objectives. The first contribution of this paper is the formalization of an event-triggered implementation of safety-critical controllers for impulsive control systems. We provide a trigger design that guarantees safety, along with the sufficient conditions for establishing the minimum inter-event time, which rules out the possibility of Zeno behavior. The second contribution is another trigger design for impulsive system that is built on the first trigger design, with the goal of imitating the key elements of a satellite maneuver. To accomplish this, we add an additional trigger condition that monitors the increase of the inter-event time of the subsequent application of control.

To demonstrate the effectiveness of the two trigger designs presented in this paper, we consider the problem of maintaining a satellite within an orbital radius range—the *satellite orbit safety problem.* For the second trigger design, we demonstrate its similarity to traditional orbit transfers. This motivates the third contribution of the paper: an event-triggered intermittent safety filter framework, which is developed as an extension of our first trigger design in the context of intermittent control systems. This framework takes inspiration from satellite maneuvers, i.e., our design is based on (1) maneuvering to safer states in order to avoid the need to filter the nominal controller, and (2) monitoring the barrier function to determine when safety is critical. Our framework actively allows a period for where nominal controller may be applied without a safety filter, and is thus able to make progress towards nominal objectives.

Notation: We denote with $\mathbb{N}$ and $\mathbb{R}$ the set of all natural and real numbers respectively. For a vector $x \in \mathbb{R}$, $\|x\|$ is its Euclidean norm. A function $\alpha : \mathbb{R} \to \mathbb{R}$ is of extended class-$\mathcal{K}$ if $\alpha(0) = 0$, and α is strictly increasing. Let $t \mapsto x(t)$ be a solution to a dynamical system for an initial condition x_0, a set $\mathcal{C}$ is forward invariant and safe if $x(t) \in \mathcal{C}$ for all time whenever $x_0 \in \mathcal{C}$.

II. Preliminaries

We begin by providing some background on the safety concept and the common practice of using safety filter, in order to motivate the problem we consider in this paper. In addition, we provide the background on event-triggered control, which we believe to be the key tool for solving our problem. Here, we consider the nonlinear system

$$\dot{x} = f(x, u) + d \tag{1}$$

where $x \in \mathbb{R}^n$ is the state, $u \in \mathbb{R}^m$ is the control input, and $d \in \mathbb{R}^n$ is the disturbance to the system. We assume throughout the paper that the disturbance is bounded, i.e., $\|d\| \le \bar{d}$.

A. Safety Formulations and Safety Filters

For safety problems, we are interested in ensuring that the states along system trajectories are not undesirable states. To address these problems, one approach is to define the safe set $\mathcal{C}$, consisting of only "safe" states via a *barrier function* $h : \mathbb{R}^n \to \mathbb{R}$ (cf. [11]) such that:

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

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

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

With a barrier function, safety problems involve finding an input signal $t \mapsto u(t)$ that ensures h always remains positive so that the safe set $\mathcal{C}$ is forward invariant, and the trajectories do not reach the undesirable states. To this end, we can use a state-feedback control $u = k(x)$ with a controller $k : \mathbb{R}^n \to \mathbb{R}^m$ satisfying the following *barrier condition*:

$$\underbrace{\left.\frac{\partial h}{\partial x}\right|_x f(x, k(x))}_{\triangleq \mathcal{L}_f h(x, k(x))} - \left\| \left.\frac{\partial h}{\partial x}\right|_x \right\| \bar{d} \ge -\alpha(h(x)). \tag{3}$$

for some extended class-$\mathcal{K}$ function α. The condition above is a conservative way to keep the function h positive. Not only does it require h to not decrease whenever it is zero, but it also requires that h does not decrease too quickly as it gets closer to zero. Nevertheless, it provides many benefits in many applications, one of which is the ability to monitor safety. We will discuss this point later in the paper.

More often than not, safety is not the only objective in control systems. To this end, a nominal controller $k_{\text{nom}} : \mathbb{R}^n \to \mathbb{R}^m$ is first designed to meet other objectives. Then to enforce the barrier condition, a safety filter defines a controller using an optimization:

$$k(x) = \underset{u\in\mathbb{R}^m}{\operatorname{argmin}} \|u - k_{\mathrm{nom}}(x)\|^2 \qquad (4)$$
$$\text{s.t.}\;\; \mathcal{L}_f h(x,u) - \left\| \frac{\partial h}{\partial x}\bigg|_x \right\| \bar{d} \geq -\alpha(h(x)).$$

The idea is that we prioritize safety above other objectives, so we adjust the nominal controller so that barrier condition is always maintained. The optimization assures that the resulting controller deviates from the nominal controller as little as possible (minimal Euclidean distance in this case).

Nevertheless, the deviation from the nominal controller when using safety filters can pose an issue because the filtered controller may no longer satisfy the original objectives. This motivates the problem we seek to address.

Consider the state-feedback control $u = k(x)$ of the nonlinear system (1). We can separate the periods when the constraint of the filter (4) is active and inactive and turn it into an intermittent nonlinear system as:

$$\dot{x} = \begin{cases} f(x, k_{\mathrm{nom}}(x)) + d, & t \in [t_i^{\mathrm{off}}, t_i^{\mathrm{on}}) \\ f(x, k(x)) + d, & t \in [t_i^{\mathrm{on}}, t_{i+1}^{\mathrm{off}}). \end{cases} \qquad (5)$$

Here, the time at which the filter is on and off is automatically determined by whether or not the constraint is active. Notice that it is possible for the off period to be nonexistent if the constraint never becomes inactive. In this work, we identify a method to assure the existence of the off period and we use event-triggered control to lengthen the off period for as long as possible.

B. Event-Triggered Sample-and-Hold Control

Event-triggered control is often studied in the context of sample-and-hold systems where it is used as a tool to reduce the frequency of control adjustments. Consider the feedback implementation of any given controller k for the nonlinear system (1) on a digital platform. The controller is not applied in a continuous fashion. Instead, the value of the controller $k(x(t_i))$ is sampled at a time instance t_i, and it is then held $u = k(x(t_i))$ until the controller next sampled again. Traditionally, this sampling is performed periodically, so the sampling time instance t_{i+1} occurs after some time has elapsed since t_i. On the other hand, under the event-triggered control framework, controls are sampled according to a *trigger condition*. Such condition is usually based on the states of the system, so the control is applied only when necessary. Trigger designs are often written as:

$$t_{i+1} = \min\left\{t \geq t_i \mid \Xi(x(t)) \leq 0\right\} \qquad (6)$$

with a trigger condition $\Xi : \mathbb{R}^n \to \mathbb{R}$ and time instance t_i when controls are applied. The trigger enforces $\Xi(x(t)) > 0$ for the duration $[t_i, t_{i+1})$ because the control is applied otherwise. Because of this useful fact, trigger conditions are often designed based on certificates like Lyapunov function or barrier function (see e.g., [13] and [23], respectively).

III. Event-Triggered Impulsive Safety

We begin the exposition with the consideration of impulsive control systems, for which we model as hybrid systems with flow dynamics $F : \mathbb{R}^n \to \mathbb{R}^n$ and a jump map $G : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$:

$$\dot{x} = F(x) + d, \qquad (7a)$$
$$x^+ = G(x, u) \qquad (7b)$$

where $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$ and $d \in \mathbb{R}^n$ are the system state, the control input, and the flow disturbance, respectively. The example for impulsive systems we will use in this paper is the satellite system, which we will give more details later.

We note importantly that sample-and-hold systems can be rewritten as impulsive control systems. For instance, consider a nonlinear system $\dot{y} = f(y, v)$ with system states $y \in \mathbb{R}^{n_y}$ and control inputs $v \in \mathbb{R}^{m_v}$. Then in the context of sample-and-hold, considering v as part of the state yields:

$$\begin{bmatrix} \dot{y} \\ \dot{v} \end{bmatrix} = \begin{bmatrix} f(y,v) \\ 0 \end{bmatrix}, \quad \begin{bmatrix} y \\ v \end{bmatrix}^+ = \begin{bmatrix} y \\ v + \Delta v \end{bmatrix}.$$

Defining the state $x = \begin{bmatrix} y & v \end{bmatrix}^\top$ and the control input $u = \Delta v = v(t_{i+1}) - v(t_i)$, we have transformed the sample-and-hold control system as an impulsive control system (7a)-(7b). Indeed, we can translate existing event-triggered control ideas to the new context. We are particularly interested in event-triggered control for safety problems in the impulsive control systems.

A. Safeguarding Impulsive Controller

For a safeguarding impulsive controller $K : \mathbb{R}^n \to \mathbb{R}^m$, we consider two following objectives. First, we require that each jump results in a state that remains in the safe set:

$$h(G(x, K(x))) \geq 0. \qquad (8)$$

Meeting this requirement is straightforward and relatively easy because the control has a direct impact to the jump map. However, we also need the states along the trajectory during the flow to meet the barrier condition:

$$\mathcal{L}_F h(x(t)) - \left\| \frac{\partial h}{\partial x}\bigg|_{x(t)} \right\| \bar{d} \geq -\alpha\big(h(x(t))\big), \qquad (9)$$

which is more problematic to satisfy. We have to rely on our control input at each jump to guarantee safety of the ensuing trajectory during the flow, up until the next jump occurrence. To address this second requirement, we build on the idea in [23] on establishing a minimum inter-event time (MIET), which is to require the controller K meets:

$$\mathcal{L}_F h(G(x, K(x))) - \left\| \frac{\partial h}{\partial x}\bigg|_{G(x,K(x))} \right\| \bar{d}$$
$$\geq -\alpha\big(h(G(x, K(x)))\big) + c. \qquad (10)$$

with some positive constant c. The idea is to use the constant c to provide a buffer so that some time has to elapse (due to continuity) after each jump, before the barrier condition (9) gets violated.

B. Event-Triggered Safeguarding Impulsive Control

We aim at reducing the frequency of the controls, and a reasonable approach is to employ event-triggered control to prescribe when to apply controls. To this end, our main trigger condition is based on monitoring the barrier condition (9). Denoting t_i as the last instance when the jump occur, we determine the jump time iteratively with:

$$t_{i+1} = \min\Big\{t \geq t_i \mid \Xi(x(t)) \leq 0\Big\}, \tag{11a}$$

$$\Xi(x) = \mathcal{L}_F h(x) - \left\| \left.\frac{\partial h}{\partial x}\right|_x \right\| \bar{d} + \alpha\big(h(x)\big). \tag{11b}$$

The trigger above makes sure that controls are applied only when necessary, i.e., when the barrier condition is violated. This strategy is a greedy approach to maximizing the times between jumps and reducing how often the jumps occur.

The main concern when relying on event-triggered control is the possibility of Zeno behavior. That is, because the elapsed time between t_i and t_{i+1} are not uniform for all $i \in \mathbb{N}$, it becomes possible that the sequence $\{t_i\}_{i\in\mathbb{N}}$ can converge to a constant value rather than infinity. This would mean there are infinite numbers of jumps in finite time, making it impractical to implement in practice.

The common approach of ruling out Zeno behavior is to establish a MIET, i.e., a common positive lower bound $\tau \leq t_{i+1} - t_i$ for all $i \in \mathbb{N}$. The task of establishing a MIET is often difficult, especially when the system is subjected to an unknown disturbance d. In this paper, we endow our controller with condition (10). This means that whenever a jump occurs, the trigger condition Ξ has a value greater than c. Thus, if the rate at which trigger condition can decrease is bounded by a constant, a MIET can be derived. A set of assumptions we can make to achieve this is given in the following result.

Proposition 1. *(Event-Triggered Safety for Impulsive Control Systems): Consider the impulsive control system* (7) *with a controller k satisfying* (8) *and* (10)*, and let the jump times $\{t_i\}_{i\in\mathbb{N}}$ be determined iteratively by the trigger design* (11)*. Assume the followings:*

(i) the flow dynamics F is bounded on $\mathcal{C}$;

(ii) the trigger condition Ξ is Lipschitz and continuously differentiable on $\mathcal{C}$.

Then there exists a MIET $\tau \leq t_{i+1} - t_i$. As a consequence, $x(t) \in \mathcal{C}$ for all time if $x_0 \in \mathcal{C}$. That is, the set $\mathcal{C}$ is safe.

Proof. Let $B \geq \|F(x)\|$ denote the bound of the flow dynamics and $L_\Xi \geq \big\| \frac{\partial \Xi}{\partial x}\big|_x \big\|$ denote the Lipschitz constant of the trigger condition. We can estimate the lower bound of the value of the trigger condition as follow:

$$\begin{aligned}\Xi(t) &= \Xi(x(t_i)) + \int_{t_i}^{t} \left.\frac{\partial \Xi}{\partial x}\right|_{x(t)} (F(x(t)) + d)dt \\ &\geq c - \int_{t_i}^{t} L_\Xi (B + \bar{d})dt \\ &= c - L_\Xi(B + \bar{d})(t - t_i).\end{aligned}$$

Hence, it is only possible for $\Xi(t) \leq 0$ when $t \geq c/(L_\Xi(B + \bar{d})) + t_i = \tau + t_i$. Therefore, $t_{i+1} - t_i \geq \tau$ and the possibility of Zeno behavior is ruled out.

Without Zeno behavior, system trajectories are defined at all time. Now note that (8) is by design of the controller, so $x(t_i) \in \mathcal{C}$ for all $i \in \mathbb{N}$. Then, we may conclude $x(t) \in \mathcal{C}$ because the barrier condition (9) is satisfied at all time due to the trigger (11). This concludes the proof. □

Proposition 1 provides an event-triggered implementation solution of an impulsive safeguarding controller. We have made two regularity assumptions in order to sufficiently establish the MIET. Even though MIET is not required for deducing safety (unlike the case of stabilization), it is important that our trigger scheme is practical, i.e., there is a big enough time separation between two consecutive control actuation. Next, we demonstrate the effectiveness of our trigger design through a satellite safety problem.

C. Application to Satellite Systems

Satellites orbiting around a central body can be described by Newton's gravitation model. Particularly, denoting the position and velocity vectors of a satellite with $\vec{r} \in \mathbb{R}^3$ and $\vec{v} \in \mathbb{R}^3$, the satellite is subjected to the dynamics from the gravity field:

$$\frac{d}{dt}\begin{bmatrix}\vec{r}\\ \vec{v}\end{bmatrix} = \begin{bmatrix}\vec{v}\\ -\frac{\mu}{r^3}\vec{r}\end{bmatrix} + \begin{bmatrix}0\\ d\end{bmatrix}$$

where μ is the gravitational parameter of the central body, r is the shorthand notation for $\|\vec{r}\|$, and $d \in \mathbb{R}^3$ is the disturbance to the dynamics such as the higher order gravity field not considered in the Newton's model.

The satellite is controlled by firing thrusters to apply a change in velocity $\Delta\vec{v}$. This change is assumed instantaneous, and a jump map is given by:

$$\begin{bmatrix}\vec{r}\\ \vec{v}\end{bmatrix}^+ = \begin{bmatrix}\vec{r}\\ \vec{v}\end{bmatrix} + \begin{bmatrix}0\\ \Delta\vec{v}\end{bmatrix}.$$

In reality, the thruster firings are not impulses; instead, they last for a few seconds. However, this timescale is much smaller than the time elapsed between each firing, which is in the scale of tens to hundreds of hours. Thus, the impulsive approximation is often used in orbital mechanics for satellite maneuvers, and we adopt this model.

We simulate an application of the impulsive trigger design (11) to the satellite system. The satellite is orbiting around an asteroid, 25143 Itokawa, and the disturbance d comes from the unmodelled higher order gravity field, which is due to the asteroid not being a perfect sphere. In term of safety, we are interested in maintaining the satellite within a range of desirable orbital distance. In our example, we want the satellite to orbit in the range $1.6R \leq r \leq 2.4R$ where R is the mean radius of the central body. The barrier function we will use is:

$$h(\vec{r}, \vec{v}) = (0.4R)^2 - (r - 2R)^2.$$

We design a safeguarding controller based on our understanding of orbital mechanics [27] of Newton's gravity model. For the reasons of space and the background needed to explain it, we omit details and reasoning in this paper. The overall explanation is that we apply impulses to inject the satellite in an orbit (without changing planes) towards the orbital radius $r_{\text{target}}(r) = 2R + 0.5(r - 2R)$ at peri/apoapsis. We place the satellite at the true anomaly that varies linearly from $-\pi$ to $-\pi/2$ (or 0 to $\pi/2$) depending on the current orbital distance.

We simulate the satellite orbiting the asteroid for 2400 hours. Fig. 2 shows the result of our simulation for the first 150 hours of satellite orbit. We report that the satellite remains within the specify safe range, and the barrier condition does not get violated. The trigger sporadically occurs for a total of 267 times across the 2400 hours, which is approximately 1 trigger every 9 hours.

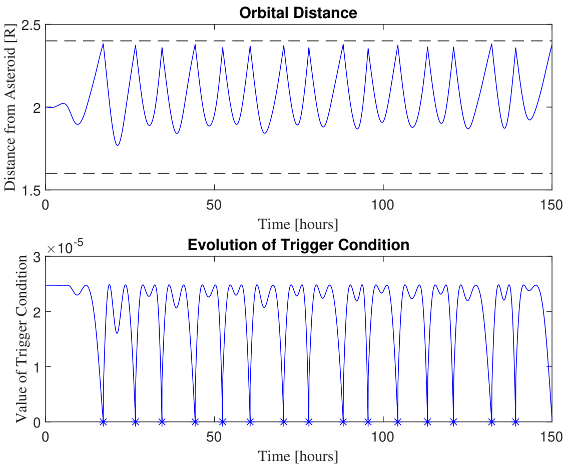

Fig. 2. [Top] Distance to the asteroid over 150 hours of satellite orbit. The plot shows the distance remains within the safe range at all time. [Bottom] Trigger condition over 150 hours of satellite orbit.

IV. Impulsive Safety Maneuvers

In this section, we investigate the concept of safety maneuvers as a way to improve the performance of event-triggered control using a barrier condition. Our idea is inspired by how satellites maneuver via orbit transfers.

A. Inspiration from Orbit Transfers

We first discuss the common practice to guarantee safety for satellites in term of maintaining within a desirable range of orbital radius. This will serve as a reference point and a motivation to our approach.

Typically, desired orbits are designed for the satellites so that they would be safe at all points along their orbits. Then to mitigate the effects from disturbances, satellite maneuvers are performed periodically, e.g. once a day, to reset the satellites back to the desired orbit. Simulations on the satellites from different initial positions on the desired orbit, i.e, Monte Carlo analyses, are performed in order to study the deviations from the desired orbits under disturbances and to ensure all safety criteria. From these analyses, an acceptable frequency of maneuvers can be found.

A satellite maneuver consists of two different impulses. The first impulse aims at repositioning the satellite to a point along the desired orbit. Once reached, a second impulse is applied to adjust the velocity in order to insert the satellite into the desired orbit. The maneuver is usually performed relatively quickly, i.e., within less than an hour for asteroid orbits. We believe there are benefits to this traditional approach, and we seek to develop our version of *safety maneuver* using event-triggered control.

B. Inter-event Time Improvement

We believe the success of the strategy relies on the improvement in inter-event time at the desired orbit. For example, in our problem of keeping a satellite within a certain range, a typical desired orbit is a circular orbit at the midpoint of the range (r=2R). Fig. 3 shows the median time at different radii, for triggers to occur after the control is applied. It should be noted that the expected inter-event time towards the center of the safe set is superior to those close to the boundary. It is cost-effective to apply two control instances (one to reposition the satellite) to enjoy the longer inter-event time.

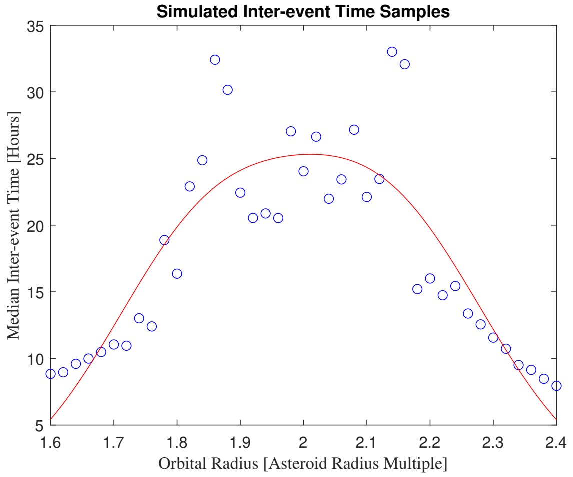

Fig. 3. We randomize 100 satellite positions at each orbital radius. For each position, we apply the impulsive safeguarding controller and collect the time it takes for the trigger to occur. The plot shows the median time values across the 100 samples at each radius.

The idea of increase in inter-event time can be abstracted in the context of barrier function. We define a function $\tau_{\text{p}} : \mathbb{R} \rightarrow \mathbb{R}$ to be such that $\tau_{\text{p}}(h(x))$ is the expected inter-event time when the control is applied at the value of barrier function $h(x)$. If we have such a function, we can find its rate of change via:

$$\dot{\tau}_{\text{p}}(x) = \left.\frac{d\tau_{\text{p}}}{dh}\right|_{h(x)} \mathcal{L}_F h(x),$$

which we can monitor along the trajectory. In the satellite example, we essentially assume $\frac{d\tau_{\text{p}}}{dh}$ is always positive, and thus, the maximum value of h translates to the longest inter-event time.

We assume the function τ_p is obtained via data collection. Much like what we have done in Fig 3, a likely scenario is that inter-event time data are collected for each value of h, and then, a curve fitting technique is performed along those data points. In the perfect scenario, the full knowledge of τ_p is preferably known as a function of state x, rather than the value of barrier function h. However, our approach uses the barrier function h as a proxy to reduce the sampling dimension and the number of samples needed. We believe this is a good strategy because h can affect inter-event time in a significant way. Referring to the trigger condition (11b), our underlying logic is that higher h will increase the value of the trigger condition Ξ, and thus, it would take longer time for it to reach zero.

Indeed, our logic is not perfectly sound. The inter-event time does not depend only on the value of the barrier function. There are many variables involved such as how fast the trigger condition changes, how $\mathcal{L}_F h$ changes with respect to h, and how much h affects the overall value of the trigger condition via α. Nevertheless, the collected data will reflect that, and the function τ_p will simply not be useful. However, if everything aligns, then we can obtain a function τ_p that we can exploit.

C. Event-triggered Impulsive Safety Maneuver

Our safety maneuver is based on monitoring a barrier condition and expected inter-event times. Each maneuver consists of two impulses. We note that, just like the satellite maneuvers, these two impulses do not need to be sampled from the same safeguarding controller. However, for simplicity, we will consider only one common safeguarding controller.

In order to maintain safety, both impulses rely on the trigger design (11). Let t_i be the last control application, the time of first impulse t_{i+1} is determined solely according to the trigger design (11). On the other hand, the second impulse is designed to be less myopic. The trigger will not wait until the violation of safety to maximize its immediate inter-event time. Instead, we allow the second impulse instance t_{i+2} to occur prematurely if continuing on will reduce expected average inter-event time. More precisely, we consider the average between the current inter-event time and the expected inter-event time after an impulse if one were to be applied:

$$\big((t - t_k) + \tau_\mathrm{p}(h(x))\big)/2.$$

To optimize the above quantity, we simply monitor the trigger condition:

$$\Xi_\tau(x) = (1 + \dot{\tau}_\mathrm{p})/2. \tag{12}$$

The trigger makes sure that we reach the local maximum point before we apply controls. However, the optimized average may be below the current expected inter-event time $\tau_\mathrm{p}(h(x(t_i)))$. To avoid this, the trigger condition Ξ_τ will only be considered after $t_{i+1} + \tau_\mathrm{p}(h(x(t_i)))$. Mathematically, our second trigger is given by:

$$t_{i+2} = \min\{t^{\text{safe}}_{i+2}, t^{\tau}_{i+2}\}, \tag{13}$$

$$t^{\text{safe}}_{i+2} = \min\big\{t \geq t_{i+1} \mid \Xi(x(t)) \leq 0\big\},$$
$$t^{\tau}_{i+2} = \min\big\{t \geq t_{i+1} + \tau_\mathrm{p}(h(x(t_{i+1}))) \mid \Xi_\tau(x(t)) \leq 0\big\}.$$

Because both triggers contain the monitoring of barrier condition, we can conclude the same safety guarantee. We state this formally as follows.

Proposition 2. *(Event-triggered Impulsive Safety Maneuvers): Consider the impulsive control system* (7) *with jump time* $\{t_i\}_{i\in\mathbb{N}}$ *determined iteratively by switching trigger designs* (11) *and* (13). *Under the same set of assumptions as in Proposition 1,* $x(t) \in \mathcal{C}$ *for all time if* $x_0 \in \mathcal{C}$. *That is, the set* $\mathcal{C}$ *is safe.* ■

We have proposed an alternative event-triggered scheme for maintaining safety in an impulsive control system. In the scheme, the trigger conditions switch between being greedy in maximizing immediate inter-event time and predicting one step ahead in term of maximizing the inter-event time. We note that the trigger scheme with only trigger design (13) can also work in term of safety guarantee, but it is unclear whether doing so will improve in term of inter-event times.

Remark 3. *(Inter-event Time Heuristic):* For our result, we can claim that the average inter-event time of two consecutive flow periods would be higher than without maneuver. However, this does not guarantee an overall increase in average inter-event time. This is because each trigger design creates a different trajectory, so it is impossible to make a guarantee on the overall average inter-event time. •

Remark 4. *(Maneuver Behavior with Safety Promoting Controller Codesign):* Our trigger scheme takes an opportunistic approach in extending the inter-event time. To fully imitate safety maneuver behavior, the first impulsive control must actively try to drive the system state to a position where the inter-event time may increase, e.g., safer location with higher value of barrier function h. This would involve a codesign of the controller—designing the controller with the expectation of using our trigger scheme. For our satellite example, we assure that each impulse would promote safety in order to take full advantage of the trigger design. In our following simulation, we demonstrate the success in imitating maneuver behavior. •

D. Simulation Result

We simulate our impulsive safety maneuver trigger scheme for the satellite safety problem explained earlier in the paper. In addition, we use the inter-event time data collected shown in Fig. 3 to fit a curve in order to estimate the function τ_p. Fig. 1 and 4 shows the results for the first 150 hours of the simulated orbital time. Safety is maintained as expected. In addition, the bottom figure shows the behavior of a safety maneuver. The trigger alternates between safety and finding the optimal location to trigger for inter-event time. Although there is no guarantee in an increase in inter-event time, we report that there are total of 215 trigger occurrences across the 2400 hours of orbital time, a reduction of 19.5 percent from the earlier simulation result.

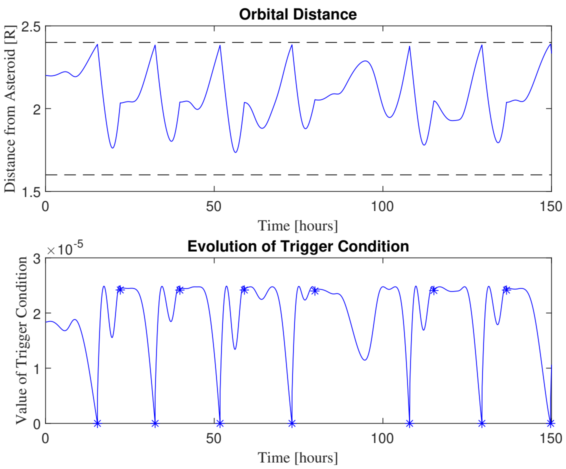

Fig. 4. Safety Maneuvers Simulation. [Top] Distance to the asteroid over 150 hours of satellite orbit. The plot shows the distance remains within the safe range at all time. [Bottom] Trigger condition over 150 hours of satellite orbit. Stars indicate the time at which the trigger occurs, showing the behavior of traditional spacecraft maneuvers.

V. Event-Triggered Intermittent Safety Filter

With the development of our event-triggered control for safety in impulsive systems, we can combine different elements from our earlier results to develop the framework for intermittent safety filter. We consider the intermittent system model for safety filter as given in (5). Here, instead of letting the time instances t_i^{off} and t_i^{on} be determined automatically based on whether the constraint of optimization (4) is active. We design different trigger conditions for switching the controller between k_{nom} and k in (4).

Our trigger scheme mimics our event-triggered safeguarding impulsive control in Section III. Recall that for impulsive systems, we use event-triggered control to monitor the barrier condition along the flow, and whenever it becomes unsafe, we apply control to jump to safety. Our idea is similar for intermittent safety filter, but instead of being able to jump directly to safety, we have periods where we apply controls to promote safety.

The first trigger condition in our scheme determines when safety is at risk and the filter needs to be back on in intermittent control system (5):

$$t_i^{\text{on}} = \min\Big\{t \geq t_i^{\text{off}} \mid \Xi_{\text{on}}(x(t)) \leq 0\Big\}, \tag{14a}$$

$$\Xi_{\text{on}}(x) = \mathcal{L}_f h(x, k_{\text{nom}}(x)) - \left\| \frac{\partial h}{\partial x}\bigg|_x \right\| \bar{d} + \alpha\big(h(x)\big). \tag{14b}$$

This trigger relies on the same idea of monitoring the barrier condition and turning the filter back on when the condition gets violated. Indeed, in order to establish the MIET of the off duration, as we have studied in the impulsive control systems in Section III, we would require that $\Xi_{\text{on}}(x(t_i^{\text{off}})) \geq c$ at time t_i^{off}. To assure this is true, we use another trigger to determine when we can turn the filter off:

$$t_{i+1}^{\text{off}} = \min\Big\{t \geq t_i^{\text{on}} \mid \Xi_{\text{off}}(x(t)) \leq 0\Big\}, \tag{15a}$$

$$\Xi_{\text{off}}(x) = \Xi_{\text{on}}(x) - c. \tag{15b}$$

The final key element in our framework is to guarantee that the above will occur. To this end, we will use the idea of increasing the value of barrier function h, which will increase the value of the trigger condition (15b). Hence, we modify the constraint filter:

$$k(x) = \underset{u \in \mathbb{R}^m}{\operatorname{argmin}} \|u - k_{\text{nom}}(x)\|^2 \tag{16}$$
$$\text{s.t.} \;\; \mathcal{L}_f h(x, u) - \left\| \frac{\partial h}{\partial x}\bigg|_x \right\| \bar{d} \geq b,$$

where $b > 0$ is a positive constant. We will simply assume that the filter is feasible, and leave feasibility as a line of future research. In any case, even with the barrier function increasing, the trigger might still not occur because the value of $L_f h(x)$ may dominate $\alpha(h(x))$. Therefore, we assume α is large enough so that the nominal controller satisfies the barrier condition, at least for a large value of h.

Assumption 5. *(Nominal Safety): Given a nominal controller k_{nom}, the function α is such that*

$$\mathcal{L}_f h(x, k_{\text{nom}}(x)) - \left\| \frac{\partial h}{\partial x}\bigg|_x \right\| \bar{d} \geq -\alpha\big(h(x)\big) + c$$

for all $x \in \mathcal{C}$ such that $h(x) \geq \bar{h}$ for some positive $\bar{h} > 0$. •

The assumption is related to the existence of a safety level (as described by h) where the nominal controller may operate without any filter. With this assumption, we assure that our safety promoting controller can drive the trajectories to such safe level, and therefore the off trigger will occur in finite time. The assumption in itself is not a strict one because a user usually gets to pick α and there always exists α large enough for the assumption to hold. Note however that the implication of choosing a large α lead to a less conservatism in safety because the trajectory is allowed to approach the boundary at a faster rate.

Now, we have all the elements for our intermittent safety filter framework. We are ready to give the following result.

Theorem 6. *(Event-triggered Intermittent Safety Filter): Consider the intermittent nonlinear system* (5) *with a nominal controller k_{nom} satisfying Assumption 5 and a safety-filtered controller given by* (16). *Let the trigger designs* (14) *and* (15) *determine the time sequences $\{t_i^{\text{on}}\}_{i\in\mathbb{N}}$ and $\{t_i^{\text{off}}\}_{i\in\mathbb{N}}$ iteratively. Then there exists t_i^{off} for every t_i^{on}. In addition, under the same set of assumptions as in Proposition 1, there exists a MIET for the off period, i.e., $\tau \leq t_{i+1}^{\text{on}} - t_i^{\text{off}}$ for all $i \in \mathbb{N}$. Consequently, $x(t) \in \mathcal{C}$ for all time if $x_0 \in \mathcal{C}$. That is, the set $\mathcal{C}$ is safe.*

Proof. First, we prove the existence of t_i^{off}. Due to the constraint in the filter (16), we can deduce $\frac{dh}{dt} \geq b$ Therefore, $\bar{h} - h(x(t_i^{\text{on}}))$ is reached in finite time $T \leq (\bar{h} - h(x(t_i^{\text{on}})))/b$. At which point, the trigger criterion (15) must already be satisfied.

The proof of MIET is as in the proof of Proposition 1. With a MIET established, we can conclude that all maximal solutions are complete, i.e., exists for all time. Then, for the time period $[t_i^{\mathrm{on}}, t_{i+1}^{\mathrm{off}})$, safety is guaranteed due to the satisfaction of constraint in the safety filter (16) where h is increasing. In addition, for the time period $[t_i^{\mathrm{off}}, t_i^{\mathrm{on}})$, safety is guaranteed due to the monitoring of the trigger condition (15b). Thus, it can be determined iteratively that $x(t) \in \mathcal{C}$ at all time if $x_0 \in \mathcal{C}$ using the barrier function h, concluding the proof. □

Theorem 6 formalizes our event-triggered intermittent safety filter framework. We summarize how our framework maintains safety as follows. We no longer use the barrier condition to filter the nominal controller. Instead, the filter aims to promote safety by increasing the barrier function in order to maneuver into states where it is possible to turn the filter off. We only use barrier condition to monitor safety and when to filter. The trigger framework effectively adds hysteresis to the system, allowing for a switching period between filtering and not filtering.

VI. Conclusion

In this paper, we have proposed various trigger designs for the purpose of reducing control effort for safety objectives. We have developed trigger schemes for safeguarding controllers in impulsive control systems and for safety filters in nonlinear systems. One particular interesting idea explored is safety maneuver which switches between actively using control effort for safety and only monitoring safety. Our future work includes the application of our event-triggered intermittent safety filter on a robotic system with the goal of accomplishing simultaneously a nominal task and collision avoidance. In addition, we will analyze the tradeoff between safety maneuver and progress towards the nominal objective, particularly in the context of the optimization-based controller with Lyapunov and barrier conditions as constraints. Our hope is that safety maneuvers will allow us to make guarantee for the satisfaction of nominal objectives.

Acknowledgement. The authors would like to thank JPL for their feedback and discussion on the control application to satellite problems. We especially thank Saptarshi Bandyopadhyay in particular for the suggestion of imitating orbit transfers and for providing the eighth-order harmonics gravity model used in our simulation results.

References

[1] T. Gurriet, A. Singletary, J. Reher, L. Ciarletta, E. Feron, and A. D. Ames, "Towards a framework for realizable safety critical control through active set invariance," in *ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*, pp. 98–106, 2018.

[2] K. Hobbs, M. Mote, M. Abate, S. Coogan, and E. Feron, "Run time assurance for safety-critical systems: An introduction to safety filtering approaches for complex control systems," *arXiv preprint arXiv:2110.03506*, 2021.

[3] A. H. De Ruiter, C. Damaren, and J. R. Forbes, *Spacecraft dynamics and control: an introduction*. New York: Wiley, 2012.

[4] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *Hybrid Systems: Computation and Control*, (Philadelphia, PA), pp. 477–492, Mar. 2004.

[5] M. Krstic and M. Bement, "Non-overshooting control of strict-feedback nonlinear systems," in *American Control Conference*, pp. 4494–4499, July 2007.

[6] P. Ögren, A. Backlund, T. Harryson, L. Kristensson, and P. Stensson, "Autonomous UCAV strike missions using behavior control Lyapunov functions," in *AIAA Guidance, Navigation, and Control Conference and Exhibit*, p. 6197, Aug. 2006.

[7] P. Wieland and F. Allgöwer, "Constructive safety using control barrier functions," *IFAC Proceedings Volumes*, vol. 40, no. 12, pp. 462–467, 2007.

[8] 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.

[9] X. Xu, P. Tabuada, J. W. Grizzle, and A. D. Ames, "Robustness of control barrier functions for safety critical control," *IFAC-PapersOnLine*, vol. 48, no. 27, pp. 54–61, 2015.

[10] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2017.

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

[12] F. Blanchini and S. Miani, *Set-Theoretic Methods in Control*. Boston, MA: Birkhäuser, 2007.

[13] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE Transactions on Automatic Control*, vol. 52, no. 9, pp. 1680–1685, 2007.

[14] 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.

[15] L. Hetel, C. Fiter, H. Omran, A. Seuret, E. Fridman, J. P. Richard, and S. I. Niculescu, "Recent developments on the stability of systems with aperiodic sampling: An overview," *Automatica*, vol. 76, pp. 309–335, 2017.

[16] M. C. F. Donkers and W. P. M. H. Heemels, "Output-based event-triggered control with guaranteed L_∞-gain and improved and decentralised event-triggering," *IEEE Transactions on Automatic Control*, vol. 57, no. 6, pp. 1362–1376, 2012.

[17] J. Chai, P. Casau, and R. G. Sanfelice, "Analysis and design of event-triggered control algorithms using hybrid systems tools," *International Journal of Robust and Nonlinear Control*, vol. 30, no. 15, pp. 5936–5965, 2020.

[18] J. Chai, P. Casau, and R. G. Sanfelice, "Analysis and design of event-triggered control algorithms using hybrid systems tools," in *IEEE Conf. on Decision and Control*, pp. 6057–6062, Dec. 2017.

[19] B. Liu, D. N. Liu, and C. X. Dou, "Exponential stability via event-triggered impulsive control for continuous-time dynamical systems," in *Chinese Control Conference*, (Nanjing, China), pp. 4056–4060, July 2014.

[20] B. Liu, D. H. J, and Z. Sun, "Stabilisation to input-to-state stability for continuous-time dynamical systems via event-triggered impulsive control with three levels of events," *IET Control Theory & Applications*, vol. 12, no. 9, pp. 1167–1179, 2018.

[21] X. Li, D. Peng, and J. Cao, "Lyapunov stability for impulsive systems via event-triggered impulsive control," *IEEE Transactions on Automatic Control*, vol. 65, no. 11, pp. 4908–4913, 2020.

[22] K. Zhang and B. Gharesifard, "Hybrid event-triggered and impulsive control for time-delay systems," *Nonlinear Analysis: Hybrid Systems*, vol. 43, p. 101109, 2021.

[23] 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.

[24] G. Yang, C. Belta, and R. Tron, "Self-triggered control for safety critical systems using control barrier functions," in *American Control Conference*, (Philadelphia, PA), pp. 4454–4459, July 2019.

[25] W. Xiao, C. Belta, and C. G. Cassandras, "Event-triggered safety-critical control for systems with unknown dynamics," in *IEEE Conf. on Decision and Control*, pp. 540–545, 2021.

[26] P. Ong, G. Bahati, and A. D. Ames, "Stability and safety through event-triggered intermittent control with application to spacecraft orbit stabilization," in *IEEE Conf. on Decision and Control*, (Cancún, Mexico), Dec. 2022. Submitted.

[27] R. R. Bate, D. D. Mueller, and J. E. White, *Fundamentals of Astrodynamics*. New York: Dover Publications, 1971.