Title

Characterizations of safety in hybrid inclusions via barrier functions

ISBN

9781450362825

Authors

Maghenem, Mohamed
Sanfelice, Ricardo G

Publication Date

2019-04-16

DOI

10.1145/3302504.3311816

Peer reviewed

Characterizations of Safety in Hybrid Inclusions via Barrier Functions

Mohamed Maghenem
University of California, Santa Cruz
mmaghene@ucsc.edu

Ricardo G. Sanfelice
University of California, Santa Cruz
ricardo@ucsc.edu

ABSTRACT

This paper investigates characterizations of safety in terms of barrier functions for hybrid systems modeled by hybrid inclusions. After introducing an adequate definition of safety for hybrid inclusions, sufficient conditions using continuously differentiable as well as lower semicontinuous barrier functions are proposed. Furthermore, the lack of existence of autonomous and continuous barrier functions certifying safety, guides us to propose, inspired by converse Lyapunov theorems for only stability, nonautonomous barrier functions and conditions that are shown to be both necessary as well as sufficient, provided that mild regularity conditions on the system's dynamics holds.

CCS CONCEPTS

• **Software and its engineering → Model checking**; • **Computer systems organization → Embedded and cyber-physical systems**;

KEYWORDS

Safety, Barrier functions, Hybrid inclusions, Hybrid systems

ACM Reference Format:
Mohamed Maghenem and Ricardo G. Sanfelice. 2019. Characterizations of Safety in Hybrid Inclusions via Barrier Functions. In *22nd ACM International Conference on Hybrid Systems: Computation and Control (HSCC '19), April 16–18, 2019, Montreal, QC, Canada.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3302504.3311816

1 INTRODUCTION

A dynamical system is said to be safe when solutions starting from a given *set of initial* conditions avoid a given *unsafe set*. In real-world applications, reaching the unsafe set can correspond to nonapplicability of a predefined feedback law [3] or, simply, to having a mobile system colliding with an obstacle that is supposed to avoid [21].

Barrier functions constitute a qualitative tool to study safety without computing the system's solutions. Generally speaking and according to [17], a barrier function candidate is a function of the system's variables which is nonpositive on the set of initial conditions and strictly positive on the unsafe set. A barrier function candidate becomes a certificate of safety when its variation along the system's solutions, which, ideally, can be expressed using infinitesimal conditions, is nonpositive, especially nearby the unsafe set. The zero sublevel set of a barrier certificate is called inductive invariant and contains the reachable set from the set of initial conditions [20].

With a slightly different approach, in [1], a barrier function candidate is defined to be positive and bounded on the set of initial conditions and unbounded when the state approaches the boundary of the unsafe set. Another slightly different definition is in [12], where a barrier function candidate is assumed to have values on the boundary of the unsafe set strictly larger than on the boundary of the initial set. Barrier functions are useful in different contexts, such as constrained optimization [24], multiagent systems [21], and constrained nonlinear control [22], to just name a few. Barrier functions are sometimes called *potential* functions [21] or, in some earlier works [8], just *Lyapunov* functions.

One of the problems related to safety analysis using barrier functions, which is less explored and not completely solved, is the converse problem. More precisely, given a safe system with respect to a given initial and unsafe sets, the converse problem pertains to finding conditions on the system's dynamics and the sets guaranteeing the existence of a barrier function certifying safety. Solutions to the converse safety problem are proposed in [18] and [25] for particular classes of continuous-time systems; namely, smooth and nonoscillatory systems in the first reference and smooth systems on compact manifolds in the second reference — see [13] for detailed comparisons. In [13], motivated by the lack of existence of a continuous barrier function depending only on the system's variables that certifies safety, time-varying barrier functions certificates are proposed for continuous-time systems. The approach in [13] is inspired from converse Lyapunov theorems for only stability ; see [15], [10], [9], and [7].

In this paper, we extend the results providing necessary and sufficient conditions of safety in [13] for hybrid systems modeled by hybrid inclusions. After introducing an adequate definition of safety for hybrid inclusions, sufficient infinitesimal conditions using barrier functions are proposed. That is, inspired by converse theorems for (non-asymptotic) Lyapunov stability [15], lower semicontinuous nonautonomous barrier functions and sufficient conditions that are also necessary are proposed. Specifically, under mild assumptions on the data defining the hybrid system, we show that the safety property is equivalent to the existence of a lower semicontinuous and nonautonomous barrier function certifying safety. To the best of our knowledge, the proposed results are unique in the field of hybrid systems and provide the first general converse characterizations for safety using barrier functions. Very importantly, due to the generality of the hybrid systems used, our results apply to both continuous-time and discrete-time systems.

This research has been partially supported by the National Science Foundation under CAREER Grant no. ECS-1450484, Grant no. ECS-1710621, and Grant no. CNS-1544396, by the Air Force Office of Scientific Research under Grant no. FA9550-16-1-0015, by the Air Force Research Laboratory under Grant no. FA9453-16-1-0053, and by CITRIS and the Banatao Institute at the University of California.

HSCC '19, April 16–18, 2019, Montreal, QC, Canada

ACM ISBN 978-1-4503-6282-5/19/04…$15.00
https://doi.org/10.1145/3302504.3311816

The remainder of the paper is organized as follows. Preliminaries, basic conditions, and supporting results are presented in Section 2. Main results including sufficient conditions as well as necessary and sufficient conditions for safety are in Section 3. Examples throughout the paper illustrate the ideas.

Due to space limitations, some proofs are omitted and will be published elsewhere.

Notations. For $x, y \in \mathbb{R}^n$, $x^\top$ denotes the transpose of x, $|x|$ the norm of x, $|x|_K := \inf_{y\in K}|x-y|$ defines the distance between x and the nonempty set $K \subset \mathbb{R}^n$, and $\langle x, y\rangle = x^\top y$ the inner product between x and y. For a set $K \subset \mathbb{R}^n$, we use $\text{int}(K)$ to denote its interior, ∂K its boundary, $\text{cl}(K)$ its closure, and $U(K)$ to denote an open neighborhood around K, namely, $\text{cl}(K) \subset U(K)$. For $O \subset \mathbb{R}^n$, $K\backslash O$ denotes the subset of elements of K that are not in O. By $\mathbb{B}$ we denote the open unit ball in $\mathbb{R}^n$ centered at the origin. For a continuously differentiable function $B : \mathbb{R}^n \to \mathbb{R}$, $\nabla B(x)$ denotes the gradient of the function B evaluated at x. By C^1 we denote the set of continuously differentiable functions. Finally, the *contingent* cone of $K \subset \mathbb{R}^n$ at $x \in \mathbb{R}^n$ is given by

$$T_K(x) := \left\{ v \in \mathbb{R}^n : \liminf_{h\to 0^+} \frac{|x+hv|_K}{h} = 0 \right\} \tag{1}$$

or, equivalently,

$$T_K(x) = \big\{ v \in \mathbb{R}^n : \exists \{h_i\}_{i\in\mathbb{N}} \to 0^+ \text{ and } \{v_i\}_{i\in\mathbb{N}} \to v : x + h_i v_i \in K \big\}. \tag{2}$$

2 PRELIMINARIES AND BASIC CONDITIONS

We consider general hybrid inclusions of the form

$$\mathcal{H} : \begin{cases} x \in C & \dot{x} \in F(x) \\ x \in D & x^+ \in G(x), \end{cases} \tag{3}$$

with the state variable $x \in \mathbb{R}^n$, the flow set $C \subset \mathbb{R}^n$, the jump set $D \subset \mathbb{R}^n$, the flow and the jump set-valued maps, respectively, $F : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ and $G : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$. See [5] for details.

A forward hybrid arc x is defined on a hybrid time domain denoted $\text{dom}\, x \subset \mathbb{R}_{\geq 0}\times\mathbb{N}$, where $\mathbb{R}_{\geq 0} := [0,\infty)$ and $\mathbb{N} := \{0,1,\ldots\}$. The forward hybrid arc x is parametrized by an ordinary time variable $t \in \mathbb{R}_{\geq 0}$ and a discrete jump variable $j \in \mathbb{N}$. Its domain of definition $\text{dom}\, x$ is such that for each $(T, J) \in \text{dom}\, x$, $\text{dom}\, x \cap ([0,T]\times\{0,1,\ldots,J\}) = \cup_{j=0}\left([t_j, t_{j+1}], j\right)$ for a sequence $\{t_j\}_{j=0}^{J+1}$, such that $t_{j+1} \geq t_j$ and $t_0 = 0$; see [5].

Similarly, x is a backward hybrid arc if and only if the function y defined as $y(t,j) := x(-t,-j)$ for each $(t,j) \in \text{dom}\, y$ with $\text{dom}\, y = -\text{dom}\, x$ is a forward hybrid arc.

Definition 1. *(forward solution to $\mathcal{H}$) A hybrid arc $x : \text{dom}\, x \to \mathbb{R}^n$ defined on a hybrid time domain $\text{dom}\, x$ and such that, for each $j \in \mathbb{N}$, $t \mapsto x(t,j)$ is absolutely continuous is a* forward solution *to $\mathcal{H}$ if*

(S0) $x(0,0) \in cl(C) \cup D$;

(S1) for all $j \in \mathbb{N}$ such that $I^j := \{t : (t,j) \in \text{dom}\, x\}$ has nonempty interior

$$\begin{aligned} &x(t,j) \in C && \text{for all} && t \in int(I^j), \\ &\dot{x}(t,j) \in F(x(t,j)) && \text{for almost all} && t \in I^j; \end{aligned} \tag{4}$$

(S2) for all $(t,j) \in \text{dom}\, x$ such that $(t, j+1) \in \text{dom}\, x$,

$$x(t,j) \in D, \qquad x(t,j+1) \in G(x(t,j)). \tag{5}$$

•

Similarly, a solution x is said to be a backward solution to $\mathcal{H}$ if there exists a forward solution y to the system $\mathcal{H}^-$ defined as

$$\mathcal{H}^- : \begin{cases} y \in C & \dot{y} \in -F(y) \\ y \in G(D) & y^+ \in G_D^{-1}(y), \end{cases} \tag{6}$$

where $G_D^{-1} : G(D) \rightrightarrows \mathbb{R}^n$ is the reciprocal of the jump map G restricted to the set D, namely,

$$G_D^{-1}(y) := \{x \in D : y \in G(x)\},$$

such that $\text{dom}\, x = -\text{dom}\, y$ and, for all $(t,j) \in \text{dom}\, y$, $x(-t,-j) = y(t,j)$.

A forward (respectively, backward) solution x to $\mathcal{H}$ starting from x_o is said to be forward (respectively, backward) complete if it is defined on an unbounded hybrid time domain; that is, the set $\text{dom}\, x$ is unbounded. It is said to be maximal if there is no forward (respectively, backward) solution z to $\mathcal{H}$ such that $x(t,j) = z(t,j)$ for all $(t,j) \in \text{dom}\, x$ with $\text{dom}\, x$ a proper subset of $\text{dom}\, z$.

Furthermore, for $x_o \in \mathbb{R}^n$, we denote by $\mathcal{S}(x_o)$ (respectively, $\mathcal{S}^-(x_o)$) the set of forward (respectively, backward) hybrid arcs starting from x_o such that:

- if $x_o \in \text{cl}(C) \cup D$, $\mathcal{S}(x_o)$ (respectively, $\mathcal{S}^-(x_o)$) is the set of forward (respectively, backward) solutions to $\mathcal{H}$ starting from $x = x_o$.
- if $x_o \in \mathbb{R}^n\backslash(\text{cl}(C)\cup D)$, $\mathcal{S}(x_o) = \mathcal{S}^-(x_o)$ reduces to the trivial hybrid arc [1] $x = x_o$ with $\text{dom}\, x = \{(0,0)\}$.

2.1 Assumptions and their impact on the system's behavior

At times we will assume the following properties for the hybrid inclusion $\mathcal{H} = (C, F, G, D)$.

(A1) Both C and D are closed subsets of $\mathbb{R}^n$.

(A2) The flow map $F : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ is outer semicontinuous [2] and locally bounded relative to C, and $F(x)$ is nonempty and convex for all $x \in C$.

(A3) The jump map $G : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ is outer semicontinuous relative to D and $G(x)$ is nonempty for all $x \in D$.

(A4) The jump map $G : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ is locally bounded relative to D.

(A5) The reciprocal jump map $G_D^{-1} : G(D) \rightrightarrows \mathbb{R}^n$ is outer semicontinuous.

(A6) The reciprocal jump map $G_D^{-1} : G(D) \rightrightarrows \mathbb{R}^n$ is locally bounded.

Conditions (A1)-(A4) are called the hybrid basic conditions. It is shown in [5] that they assure very useful properties on the system's forward solutions. As we state next, some of these repercussions extend to the backward solutions, under the additional assumptions (A5)-(A6). These properties will play a central role in proving the converse results for safety in terms of barrier functions in Section 3.3.

Definition 2 (Local eventual boundedness [5]). *A sequence of hybrid arcs $x_i : \text{dom}\, x_i \to \mathbb{R}^n$, $i = 1, 2, \ldots$, is said to be locally eventually bounded if, for any $m > 0$, there exists $i_o > 0$ and $M > 0$ such that for all $i > i_o$, all $(t,j) \in \text{dom}\, x_i$ with $|t+j| < m$, $|x_i(t,j)| \leq M$.*

•

[1] Such hybrid arcs are not solutions.

[2] The set-valued map F is said to be outer semicontinuous if for all $x \in \mathbb{R}^n$ and all sequences of points $\{x_i\}_{i=0}^\infty$ and $\{y_i\}_{i=0}^\infty$ such that $x_i \to x$, $y_i \in F(x_i)$ and $y_i \to y$ for some $y \in \mathbb{R}^n$, we have $y \in F(x)$. Equivalently, F is outer semicontinuous if and only if the graph of F is closed [19, Theorem 5.7] (see also [5]).

Lemma 2.1. *Suppose (A1)-(A2) and (A5) hold. Let the sequence of backward hybrid arcs $\{x_i\}_{i=0}^{\infty}$ with $x_i \in \mathcal{S}^-(x_{io})$ and $x_{io} \in \mathbb{R}^n$ for all $i \in \mathbb{N}$, be locally eventually bounded. Then, the following hold:*

1) *There exists a subsequence $\{x_{i_l}\}_{l=0}^{\infty}$ of $\{x_i\}_{i=0}^{\infty}$ graphically converging to a backward hybrid arc $x \in \mathcal{S}^-(x_o := \lim_{l\to\infty} x_{i_l o})$.*
2) *For all $(T, J) \in \mathbb{R}_{\geq 0} \times \mathbb{N}$ and $\epsilon > 0$, there exists $l_o \in \mathbb{N}$ such that, for all $l > l_o$, the hybrid arc x and x_{i_l} obtained from 1) are (T, J, ϵ)-close, namely:*
   (a) *$\forall (t, j) \in \operatorname{dom} x$, $t \geq -T$ and $j \geq -J$, there exists s such that $(s, j) \in \operatorname{dom} x_{i_l}$, $|t - s| < \epsilon$, and $|x(t, j) - x_{i_l}(s, j)| < \epsilon$,*
   (b) *$\forall (t, j) \in \operatorname{dom} x_{i_l}$, $t \geq -T$ and $j \geq -J$, there exists s such that $(s, j) \in \operatorname{dom} x$, $|t - s| < \epsilon$, and $|x(s, j) - x_{i_l}(t, j)| < \epsilon$.*

The proof of Lemma 2.1 is based on [5, Theorem 6.1, Theorem 6.8, and Theorem 5.25].

Lemma 2.2. *Suppose (A1)-(A2) and (A5)-(A6) hold. Assume that all the backward solutions starting from a compact set $K \subset C \cup D$ are bounded or complete. Then, each sequence of backward solutions, starting from K, is locally eventually bounded.*

Proof. The proof is a straightforward consequence of [5, Proposition 6.13]. □

2.2 Monotonicity along differential inclusions

This section recalls elements needed to formulate necessary and sufficient infinitesimal conditions guaranteeing the monotonicity of lower semicontinuous functions along solutions of differential inclusions — see [4, Theorem 6.3].

Definition 3 (Lower semicontinuous functions). *A function $B : \mathbb{R}^n \to \mathbb{R}$, is said to be lower semicontinuous at $x \in \mathbb{R}^n$ if, for each sequence $\{x_n\}_{n=0}^{\infty} \subset \mathbb{R}^n$ with $\lim_{n\to\infty} x_n = x$, we have $\lim_{n\to\infty} B(x_n) \geq B(x)$. The function B is said to be lower semicontinuous if it is lower semicontinuous at each $x \in \mathbb{R}^n$.* •

Next, we use the characterization in [4, Theorem 2.5] to define the proximal subdifferential for a lower semicontinuous function.

Definition 4 (Proximal subdifferential). *The proximal subdifferential of a lower semicontinuous function $B : \mathbb{R}^n \to \mathbb{R}$ is the set valued map $\partial_P B : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ such that, for all $x \in \mathbb{R}^n$,*

$$\partial_P B(x) := \big\{\zeta \in \mathbb{R}^n : \exists U(x),\ \exists \epsilon > 0 : \forall y \in U(x) \\ B(y) \geq B(x) + \langle \zeta, y - x\rangle - \epsilon |y - x|^2\big\}. \quad (7)$$

Moreover, each vector $\zeta \in \partial_P B(x)$ is said to be a proximal subgradient of B at x. •

If B is C^2 at $x \in \operatorname{dom} B$, that is, ∇B exists and is C^1 at x, then $\partial_P B(x) = \{\nabla B(x)\}$. Moreover, the latter equality holds also when B is only C^1 provided that $\partial_P B(x) \neq \emptyset$ — see [4, Theorem 5.7 and Corollary 2.6].

Definition 5. *A set-valued map $F : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ is said to be locally Lipschitz if for each compact set $K \subset \mathbb{R}^n$ there exists $k > 0$ such that, for all $x \in K$ and $y \in K$,*

$$F(y) \subset F(x) + k|x - y|\mathbb{B}. \quad (8)$$

•

In the following lemma, we present necessary and sufficient infinitesimal conditions for a lower semicontinuous function to be nonincreasing, inside an open set, along solutions to a differential inclusion. This result is a small generalization of [4, Theorem 6.3] since the linear growth condition on the flow map is not required.

Lemma 2.3. *Suppose $B : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ is locally bounded and lower semicontinuous. Assume that the set-valued map F, defining the differential inclusion $\dot{x} \in F(x)$, satisfies (A2) and is locally Lipschitz. Then, for each solution $t \mapsto x(t)$ to $\dot{x} \in F(x)$, $t \mapsto B(x(t))$ is nonincreasing if and only if*

$$\langle \zeta, \eta\rangle \leq 0 \qquad \forall \zeta \in \partial_P B(x),\ \forall \eta \in F(x),\ \forall x \in \mathbb{R}^n. \quad (9)$$

Remark 1. We stress that the original statement in [4, Theorem 6.3] assumes that F is upper semicontinuous, locallay Lipschitz and having convex and compact images. Such a requirement is equivalent to (A2). Indeed, outer semicontinuous mappings have closed images, if additionally, are locally bounded, their images are compact [6]. Furthermore, outer semicontinuous and locally bounded mappings are upper semicontinuous [2, Proposition 1.4.8]. Conversely, locally Lipschitz maps are locally bounded, and upper semicontinuous maps with closed images are outer semicontinuous [5, Theorem 6.3]. •

Next, we propose necessary conditions for a lower semicontinuous function to be nonincreasing inside a closed set C, along solutions to a differential inclusion $\dot{x} \in F(x)$. Those conditions do not require the linear growth condition imposed in [4, Theorem 6.3]. Furthermore, under extra conditions on the boundary of the closed set C, the following result extends the necessity part of Lemma 2.3.

Lemma 2.4. *Suppose $B : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ is locally bounded and lower semicontinuous, and the set-valued map F satisfies (A2). Furthermore, assume that*

(A7) for each $x_o \in \partial C$, if $F(x_o) \cap T_C(x_o) \neq \emptyset$, then, for each $v_o \in F(x_o) \cap T_C(x_o)$, there exists a continuous function $v : \partial C \cap U(x_o) \to \mathbb{R}^n$ such that $v(x_o) = v_o$ and $v(x) \in F(x) \cap T_C(x)$ for all $x \in C \cap U(x_o)$.

Then, for a closed set $C \subset \mathbb{R}^n$ and for each solution $t \mapsto x(t)$ to $\dot{x} \in F(x)$ such that $x(\operatorname{dom} x) \subset C$, $t \mapsto B(x(t))$ is nonincreasing only if

$$\langle \zeta, \eta\rangle \leq 0 \qquad \forall \zeta \in \partial_P B(x),\ \forall \eta \in F(x) \cap T_C(x),\ \forall x \in C. \quad (10)$$

Remark 2. Roughly speaking, Assumption (A7) ensures the existence of a nontrivial solution x to $\dot{x} \in F(x)$ along each vector field in $F \cap T_C$. The latter requirement is important since the inequality in (10) needs to hold for any vector field in $F \cap T_C$ based on the variations of the function $t \mapsto B(x(t))$ with x solution to $\dot{x} \in F(x)$. If $F \cap T_C$ is lower semicontinuous and T_C is convex, (A7) holds for free via Michæl Selection Theorem [14]. •

Remark 3. It is important to notice that, when the solutions to $\dot{x} \in F(x)$ are defined in a closed set, condition (10) fails to be sufficient when B is a general lower semicontinuous function. However, it becomes sufficient for monotonicity when it holds on a neighborhood of C instead of only on the set C or under extra regularity conditions. •

3 MAIN RESULTS

3.1 Safety in hybrid inclusions

Given a hybrid system $\mathcal{H} = (C, F, D, G)$ and two sets $X_o \subset \mathrm{cl}(C) \cup D$ and $X_u \subset \mathbb{R}^n$, we introduce a safety notion that extends the one proposed in [17] to the general setting of hybrid inclusions. By convention, points not in $\mathrm{cl}(C) \cup D$ are considered unsafe, which implies that $\mathbb{R}^n \backslash (\mathrm{cl}(C) \cup D) \subset X_u$.

Definition 6 (Safety). *The hybrid system $\mathcal{H}$ is said to be safe with respect to the initial set X_o and the unsafe set X_u, where $X_o \cap$*

$X_u = \emptyset$, if each solution x starting from $x_o \in X_o$ satisfies $x(t,j) \in \mathbb{R}^n \backslash X_u$ for all $(t,j) \in \operatorname{dom} x$. •

3.2 Sufficient conditions for safety using barrier functions

A barrier function candidate with respect to the initial and the unsafe sets (X_o, X_u) is defined as follows.

Definition 7. *A function $B : \mathbb{R}^n \to \mathbb{R}$ is said to be a barrier function candidate for safety with respect to (X_o, X_u) if*

$$\begin{aligned} B(x) &> 0 \qquad \forall x \in X_u \cap (cl(C) \cup D) \\ B(x) &\leq 0 \qquad \forall x \in X_o. \end{aligned} \tag{11}$$

•

Furthermore, we introduce the following set that will be used in the statements and the proofs:

$$K_e := \left\{ x \in \mathbb{R}^n : B(x) \leq 0 \right\}. \tag{12}$$

It is immediate to notice that $X_o \subset K_e$ and that $X_u \cap (C \cup D) \cap K_e = \emptyset$.

Lemma 3.1. *When the barrier candidate B is lower semicontinuous, the set K_e is closed.*

Proof. Using contradiction, we assume that K_e is not closed. Hence, there exists $y \in \mathbb{R}^n$ and a sequence $\{y_i\}_{i \in \mathbb{N}} \to y$ such that $y_i \in K_e$ for all $i \geq 0$ and $y \notin K_e$. The latter fact implies, after passing to a subsequence, that $\lim_{i \to \infty} B(y_i) \leq 0 < B(\lim_{i \to \infty} y_i) = B(y)$. The later contradicts the lower semicontinuity of B. □

Before establishing sufficient conditions for safety, we state the following general fact.

Fact. Consider the hybrid inclusion $\mathcal{H} = (C, F, D, G)$ and a closed set $K \subset C \cup D$. If a (forward) solution x starting from $x_o \in K$ leaves the set K, then it has to be under one of the two following scenarios.

(Sc1) The solution x leaves the set K after a jump. This implies the existence of $(t,j) \in \operatorname{dom} x$ such that $x(t,j) \in K \cap D$ and $(t, j+1) \in \operatorname{dom} x$ with $x(t, j+1) \notin K$ and $x(t, j+1) \in G(x(t,j))$.

(Sc2) The solution x leaves the set K by flowing. This implies the existence of $t_2' > t_1' \geq 0$ and $j \in \mathbb{N}$ such that $([t_1', t_2'], j) \subset \operatorname{dom} x$ and $x((t_1', t_2'), j) \subset (U(\partial K) \backslash K) \cap C$, with $x(t_1', j) \in \partial K$ and $x(t_2', j) \notin K$.

•

When K is not closed, the case in (Sc2) is replaced by

(Sc3) The solution x leaves the set K by flowing. It implies the existence of $t_2' > t_1' \geq 0$ and $j \in \mathbb{N}$ such that $([t_1', t_2'], j) \subset \operatorname{dom} x$ and either $x((t_1', t_2'), j) \subset (U(\partial K) \backslash K) \cap C$, with $x(t_1', j) \in \partial K$ and $x(t_2', j) \notin K$, or $x([t_1', t_2'), j) \subset K$, with $\lim_{t - t_2' \to 0^-} x(t,j) \in \operatorname{cl}(K) \backslash K$. In the second case, the solution x dies on the boundary ∂K.

Theorem 3.2. *Given a hybrid system $\mathcal{H}$, assume that (A2) holds and $G(x) \neq \emptyset$ for all $x \in D$. Consider a $\mathcal{C}^1$ barrier function candidate B with respect to the initial and the unsafe sets (X_o, X_u) as in (11). Then, the hybrid system $\mathcal{H}$ is safe with respect to (X_o, X_u) if*

$$\langle \nabla B(x), \eta \rangle \leq 0 \qquad \forall x \in (U(\partial K_e) \backslash K_e) \cap C \text{ and } \forall \eta \in F(x) \cap T_C(x), \tag{13}$$

$$B(\eta) \leq 0 \qquad \forall \eta \in G(x) \quad \forall x \in D \cap K_e, \tag{14}$$

$$G(x) \subset C \cup D \qquad \forall x \in D \cap K_e. \tag{15}$$

Proof. From the definition of the set K_e in (12) and using Lemma 3.1, we conclude that K_e is closed and at the same time $K_e \cap (C \cup D)$ is also closed. That is, the statement is proved if we show that the closed set $K_e \cap (C \cup D)$ is forward pre-invariant, namely, all the maximal solutions starting from $K_e \cap (C \cup D)$ remain in it. Indeed, under the forward pre-invariance of the closed set $K_e \cap (C \cup D)$, we conclude that $B(x(t,j)) \leq 0$ and $x(t,j) \in C \cup D$ for all $(t,j) \in \operatorname{dom} x$ and for each solution x starting from $K_e \cap (C \cup D)$. Hence, since $X_o \subset K_e \cap (C \cup D)$, the solutions starting from X_o cannot reach the set X_u where the barrier function B is strictly positive, thus, Theorem 3.2 is proved.

So, we show forward pre-invariance of the closed set $K := K_e \cap (C \cup D)$ under (13)-(15). To reach a contradiction, let us assume that (13)-(15) hold and the set K is not forward pre-invariant. That is, there exist a maximal solution x starting from $x_o \in K$ that leaves the set K following one of the scenarios (Sc1) and (Sc2).

- Assume that the solution x leaves the set K after a jump from K to $\mathbb{R}^n \backslash K$ following the scenario (Sc1). This implies, using (15) and the definition of B, that $B(x(t, j+1)) > 0$ with $x(t, j+1) \in G(x(t,j))$. However, $x(t,j) \in K \cap D$, hence using (14), it follows that $B(x(t, j+1)) \leq 0$ for all $x(t, j+1) \in G(x(t,j))$. The latter fact yields to a contradiction.
- Assume that the solution x leaves the set K by flowing under the scenario (Sc2). We conclude, in this case that $B(x(t,j)) > 0$ for all $t \in (t_1', t_2']$ and $x((t_1', t_2'], j) \subset (U(\partial K) \backslash K) \cap C$, where t_1' and t_2' are as in (Sc2). Furthermore, we first show that $\dot{x}(t,j) \in T_C(x(t,j))$ for almost all $t \in [t_1', t_2']$. Indeed, let $t \in (t_1', t_2')$ such that $\dot{x}(t,j)$ exists and satisfies $\dot{x}(t,j) \in F(x(t,j))$. Moreover, let a sequence $\{t_n\}_{\mathbb{N}} \subset (0, t_2' - t)$ such that $t_n \to 0$. That is, for $v_n(t) := (x(t_n, j) - x(t,j))/t_n$, we have $\lim_n v_n(t) = \dot{x}(t,j)$ and at the same time $x(t,j) + t_n v_n(t) = x(t_n, j) \in C$. Hence, using (2), we conclude that $\dot{x}(t,j) \in T_C(x(t,j))$. Next, since the function B is assumed to be continuously differentiable and the solution $x(\cdot, j)$ is absolutely continuous on the interval $[t_1', t_2']$, it follows that $B(x(\cdot, j))$ is also absolutely continuous on that interval. Hence,

$$B(x(t_2', j)) - B(x(t_1', j)) = \int_{t_1'}^{t_2'} \langle \nabla B(x(t,j)), \dot{x}(t,j) \rangle dt > 0, \tag{16}$$

where $\dot{x}(t,j) \in F(x(t,j)) \cap T_C(x(t,j))$ for almost all $t \in [t_1', t_2']$. However, $x((t_1', t_2'], j) \subset (U(\partial K) \backslash K) \cap C$ and using (13) we conclude that, for all $t \in (t_1', t_2')$, $\langle \nabla B(x(t,j)), \eta \rangle \leq 0$ for all $\eta \in F(x(t,j)) \cap T_C(x(t,j))$, which implies that $B(x(t_2', j)) - B(x(t_1', j)) \leq 0$. Hence, the contradiction with (16) follows.

□

Example 1. Consider the hybrid system

$$\begin{aligned} F(x) &:= \begin{bmatrix} -x_2 x_1 \\ -(|x|^2 - [0,1])(|x|^2 - \frac{1}{2})(2 - |x|^2) \end{bmatrix} \quad \forall x \in C, \\ C &:= \left\{ x \in \mathbb{R}^2 : x_2 \geq 0,\ x_1 \in [-1, 1] \right\}, \\ G(x) &:= [0,1] \begin{bmatrix} x_2 \\ |x_1| \end{bmatrix} \quad \forall x \in D, \\ D &:= \left\{ x \in \mathbb{R}^2 : x_2 = 0,\ |x| \leq 1 \right\}. \end{aligned}$$

We would like to verify, using Theorem 3.2, that the system is safe with respect to the sets

$$X_o := \left\{ x \in C \cup D : |x|^2 \leq 1/4,\ x_2 \geq 0 \right\}, \tag{17}$$

$$X_u := \{ x \in C \cup D : x_2 \geq 3 \} \cup (\mathbb{R}^n \backslash (C \cup D)). \tag{18}$$

That is, we start introducing the C^1 barrier function candidate

$$B(x) := x_2(|x|^2-1). \tag{19}$$

Indeed, it is easy to see that, for each $x \in X_o$, we have $B(x) \leq -1/2x_2 \leq 0$ since x_2 is always positive in $C \cup D$. Moreover, for each $x \in X_u \cap (C \cup D)$, we have $x_2 \geq 3$ hence $B(x) \geq 24 > 0$. Furthermore, according to (12), the set

$$K_e \cap (C \cup D) = \left\{x \in C \cup D : |x|^2-1 \leq 0,\ x_2 \geq 0\right\}$$

is closed.

Before verifying the safety conditions in Theorem 3.2, we notice that the set X_o is not forward pre-invariant, namely, the system admits solutions starting from X_o that actually leave X_o. The same fact holds for the set $\mathbb{R}^n \backslash X_u$. Indeed, for each $x \in X_o$ such that $|x| = 1/4$ there exists $\eta \in F(x)$ such that $\eta_2 > 0$ which implies the existence of a solution starting from X_o and flowing outside the latter set. Also, for each $x_o = [0\ \alpha]^\top$ ($\alpha \geq 2$) and for all $\eta \in F(x_o)$, we have $\eta_2 > 0$; hence, there exists a solution flowing from $[0\ 2]^\top \notin X_u$ and reaching $X_u \cap (C \cup D)$ after finite time. This being said, we are still able to conclude safety with respect to (X_o, X_u) using Theorem 3.2. Indeed, the set $(U(\partial K_e) \backslash K_e) \cap C$ can be chosen as $(U(\partial K_e) \backslash K_e) \cap C = \{x \in C : |x_1| \leq 1,\ |x| \in (1, 2)\}$. Then, simple computations allow us to conclude that for all x in the latter set, (13) holds. Furthermore, for all $x \in D \cap K_e$, $G(x) \subset C \cup D$; hence, (15) holds. Moreover, simple computations confirm that after each jump from the set $K \cap D$, B remains nonpositive, which implies that (14) holds. Thus, the system is safe. □

In the following result we provide an alternative characterization for safety when the barrier candidate is only lower semicontinuous. Thanks to Lemma 2.3, we are able to combine infinitesimal flow conditions to jump conditions using a not necessarily smooth barrier function candidate.

Theorem 3.3. *Given a hybrid system $\mathcal{H}$, assume that (A2) holds and $G(x) \neq \emptyset$ for all $x \in D$. Let the flow map F be locally Lipschitz and the set X_o be closed. Then, the system $\mathcal{H}$ is safe with respect to (X_o, X_u) if there exists a lower semicontinuous barrier function candidate B with respect to (X_o, X_u) such that*

$$B(\eta) \leq 0 \qquad \forall \eta \in G(x),\ \forall x \in D \cap K_e, \tag{20}$$

$$G(x) \subset C \cup D \qquad \forall x \in D \cap K_e, \tag{21}$$

$$\langle \zeta, \eta \rangle \leq 0 \qquad \forall \zeta \in \partial_P B(x),\ \forall \eta \in F(x),\ \textit{and}\ \forall x \in U(\partial K_e \cap C) \backslash K_e. \tag{22}$$

Proof. Using Lemma 3.1 under the lower semicontinuity of B, we conclude that the set $K := K_e \cap (C \cup D)$ is closed. Hence, the statement is proved, as in Theorem 3.2, if we show forward pre-invariance of the closed set K. Using contradiction, we assume that (20)-(22) hold and, at the same time, the set K is not forward pre-invariant. Indeed, two situations are possible. First, we assume the existence of a solution x starting from the set K that leaves the set K after jumping from the set K to its complement following the scenario (Sc1). The contradiction, in this case, can be shown using the same argument as in the proof of Theorem 3.2. Next, we assume the existence of a solution x starting from K and leaves the set K by flowing under the scenario (Sc2). This latter fact implies that $B(x(t_1', j)) = 0$ and $B(x(t, j)) > 0$ for all $t \in (t_1', t_2']$ and $x((t_1', t_2'], j) \subset (U(\partial K) \backslash K) \cap C \subset U(\partial K_e \cap C) \backslash K_e$ where t_1' and t_2' are introduced in (Sc2). Furthermore, since the function B is lower semicontinuous, Lemma 2.3 applies to conclude that, under (22), B is nonincreasing along the system's flows lying in $U(\partial K_e \cap C) \backslash K_e$. Thus, a contradiction with (Sc2) follows. □

The previous result can be useful when the set of initial conditions X_o is disconnected. Indeed, in this case, we have $X_o = \cup_{i=1}^{I} X_{oi}$ with $I > 0$ and $X_{oi} \cap X_{oj} = \emptyset$ if $i \neq j$. Assume further the existence of a smooth barrier candidate B_i with respect to each (X_{oi}, X_u) as in (11). In this setting, there exists a not necessarily smooth barrier candidate B with respect to (X_o, X_u) such that $B(x) = B_i(x)$ with i selected based on the location of x with respect to $X_{o1}, X_{o2}, ..., X_{oI}$. The later fact is illustrated in the following example.

Example 2. Consider the hybrid system

$$F(x) := [0, 1] \begin{bmatrix} x_2 x_1 \\ -x_1^2 \end{bmatrix} \ \forall x \in C,$$

$$C := \left\{x \in \mathbb{R}^2 : x_2 \geq 0,\ x_1 \in [-4, 4]\right\},$$

$$G(x) := [0, 1] \begin{bmatrix} -x_1 \\ 0 \end{bmatrix} \ \forall x \in D,$$

$$D := \left\{x \in \mathbb{R}^2 : x_2 = 0,\ -3 \leq x_1 \leq -1\right\}.$$

We would like to verify, using Theorem 3.3, that the system is safe with respect to the sets

$$X_o := \{x \in C : |[(x_1 - 2) \quad x_2]| \leq 1,\ |[(x_1 + 2) \quad x_2]| \leq 1/2\}, \tag{23}$$

$$X_u := \{x \in C \cup D : x_2 \geq 3\} \cup (\mathbb{R}^n \backslash (C \cup D)). \tag{24}$$

We start introducing the barrier function candidate

$$B(x) := \begin{cases} |[(x_1 - 2) \quad x_2]|^2 - 4 & \text{if } x_1 \geq 0, \\ |[(x_1 + 2) \quad x_2]|^2 - 1 & \text{otherwise.} \end{cases} \tag{25}$$

It is easy to see that the candidate B is discontinuous on the set $S := \{x \in C : x_1 = 0\}$. Moreover, it is lower semicontinuous at each element in the set S and continuously differentiable elsewhere. In fact its proximal subdifferential is

$$\partial_P B(x) = \begin{cases} \left\{[2(x_1 - 2) \quad 2x_2]^\top\right\} & \text{if } x_1 > 0, \\ \left\{[2(x_1 + 2) \quad 2x_2]^\top\right\} & \text{if } x_1 < 0, \\ \left\{[1, \infty)[-4 \quad 2x_2]^\top\right\} & \text{if } x \in S. \end{cases} \tag{26}$$

It is easy to see that, for each $x \in X_o$, if $x_1 \geq 0$ then $B(x) \leq -3$; otherwise, $B(x) \leq -3/4$. Moreover, for each $x \in X_u \cap (C \cup D)$, we have $x_2 \geq 3$ hence $B(x) \geq 1 > 0$. Furthermore, according to (12), the set

$$K_e \cap (C \cup D) = \left\{x \in C : \begin{bmatrix} |[(x_1 - 2) \quad x_2]|^2 \leq 4 & \text{if } x_1 \geq 0, \\ |[(x_1 + 2) \quad x_2]|^2 \leq 1 & \text{otherwise} \end{bmatrix}\right\}$$

is closed. To conclude safety with respect to the sets (X_o, X_u) using Theorem 3.3, we start noticing that

$$\langle \zeta, \eta \rangle \in \begin{cases} -4[0, 1] x_1 x_2 & \text{if } x_1 > 0, \\ 4[0, 1] x_1 x_2 & \text{if } x_1 < 0, \\ \{0\} & \text{if } x \in S \end{cases} \tag{27}$$

for all $\zeta \in \partial_P B(x)$ and for all $\eta \in F(x)$. Hence, (22) is satisfied for all $x \in \mathbb{R}^n$. Furthermore, for all $x \in D \cap K_e = D$, $G(x) \subset [[0, 3] \quad 0]^\top \subset C \cup D$; hence, (21) holds. Moreover, $B(\eta) \leq 0$ for all $\eta \in G(x) \subset [[0, 3] \quad 0]$, which implies that (20) holds. Thus, the system is safe. □

Remark 4. The results presented in this section are extensions to the safety framework proposed in [16, 17, 23] to general hybrid inclusions. In the existing literature, the most general class of dynamical systems that has been considered in the context of safety

is the class of hybrid automata [17]. According to the latter reference, a safe and an unsafe sets are associated to each functioning mode of the system, and the sets can be different from one mode to another. Furthermore, each mode is governed by a differential equation and the state variable is allowed to jump each time the mode switches. According to this setting, the safety property is guaranteed using multiple barrier functions where each barrier function is associated to one mode and satisfies a condition similar to (11). Furthermore, a flow condition similar to (13) is assumed to hold along each mode using the appropriate barrier candidate and system's dynamics. Moreover, a jump condition similar to (14) has to hold to guarantee that after each switch or change of mode the barrier candidate associated to the new mode is nonpositive after the jump. In our case, the system's dynamics are more general and the jumps are not necessarily synchronized with the switch in the flow modes. Consequently, it is not possible to decompose the safe and the unsafe sets according to distinct modes. •

3.3 Necessary and sufficient conditions for safety using barrier functions

In this section, inspired by converse theorems for (non-asymptotic) Lyapunov stability, we formulate necessary and sufficient conditions for safety in hybrid inclusions. Converse theorems for (non-asymptotic) Lyapunov stability have been studied during the 40-50's by the eastern control community, see [7, 9–11, 15], and recently extended to the safety context in [13] for continuous-time systems. In the latter reference, inspired from [7, Example 21.14, page 82] and [9, Remark, Page 46], it has been shown that there exist systems that are safe but do not admit an autonomous and continuous barrier function candidate guaranteeing their safety, see [13, Example 2]. As a remedy to this fact, time-varying barrier functions and sufficient conditions for safety that are also necessary are proposed in [13] for continuous-time systems. In this section we extend the main results in [13] to general hybrid inclusions. Under assumptions (A1)-(A6), we show that the existence of a lower semicontinuous and nonautonomous barrier function candidate satisfying some conditions is equivalent to safety as formulated in Definition 6.

Theorem 3.4. *Given a hybrid system $\mathcal{H}$, assume that (A1)-(A6) hold. Let the set X_o be closed and suppose that every maximal backward solution is bounded or complete. Then, the system $\mathcal{H}$ is safe with respect to (X_o, X_u) if and only if there exists a barrier function $B : \mathbb{R}_{\geq 0} \times \mathbb{N} \times \mathbb{R}^n \to \mathbb{R}$ such that, uniformly in k, $(t, x) \mapsto B(t, k, x)$ is lower semicontinuous, B is nonincreasing along the flows of $\mathcal{H}$, and the following conditions hold:*

$$B(t,k,x) \leq 0 \qquad \forall (t,k,x) \in \mathbb{R}_{\geq 0} \times \mathbb{N} \times X_o, \tag{28}$$

$$B(t,k,x) > 0 \qquad \forall (t,k,x) \in \mathbb{R}_{\geq 0} \times \mathbb{N} \times (X_u \cap (C \cup D)), \tag{29}$$

$$B(t,k+1,\eta) \leq 0 \qquad \forall \eta \in G(x) \text{ and } \forall (t,k,x) \in K_e \cap (\mathbb{R}_{\geq 0} \times \mathbb{N} \times D), \tag{30}$$

$$G(x) \subset C \cup D \qquad \forall x \in D \text{ s.t. } (t,k,x) \in K_e \text{ for some } (t,k) \in \mathbb{R}_{\geq 0} \times \mathbb{N}, \tag{31}$$

$$\text{where} \quad K_e := \left\{(t,k,x) \in \mathbb{R}_{\geq 0} \times \mathbb{N} \times \mathbb{R}^n : B(t,k,x) \leq 0\right\}. \tag{32}$$

Moreover, if additionally (A7) holds and the flow map F is locally Lipschitz, the barrier function B satisfies [3]

$$\theta + \langle \zeta, \eta \rangle \leq 0 \qquad \forall \eta \in F(x) \cap T_C(x), \ \forall (\theta, \zeta) \in \partial_P B(\cdot,k,\cdot)(t,x), \text{ and } \forall (t,k,x) \in \mathbb{R}_{\geq 0} \times \mathbb{N} \times C. \tag{33}$$

Proof. In order to prove the sufficient part of the statement, we will first show that $(t,k) \mapsto B(t,k,x(t,k))$ is non-positive for all $(t,k) \in \operatorname{dom} x$ and for all $x \in \mathcal{S}(X_o)$. Indeed, in the opposite scenario we will allow to have $x(t,k) > 0$ for some $(t,k) \in \operatorname{dom} x$ and for some $x \in \mathcal{S}(X_o)$ possibly leading to $x(t,k) \in X_u \cap (C \cup D)$. Since B is nonincreasing along the flows, we conclude for each solution x to $\mathcal{H}$ with $(0,k,x(0,k)) \in K_e$, $B(t,k,x(t,k))$ remains non-positive during the flows; thus $(t,k,B(t,k))$ remains in K_e. Furthermore, after any possible jump from $(t,k,x(t,k)) \in K_e$, under (30), B remains non positive; thus $(t,k+1,x(t,k+1))$ remains in K_e after the jump. Hence, applying the same argument recursively, each solution $x \in \mathcal{S}(X_o)$ starting from X_o satisfies $(t,k,x(t,k)) \in K_e$ from all $(t,k) \in \operatorname{dom} x$. In order to complete the proof, it remains to show that all the maximal solutions starting from X_o remain in $C \cup D$ so, that then, they do not jump to $X_u \backslash (C \cup D)$. Since the sets C and D are both closed, the only way for a solution starting from X_o to leave the set $C \cup D$ is after a jump. The latter behavior is prevented by (31). Indeed, for each $y \in D$ reached by a solution x starting from X_o, $x(t,k) = y$ for some $(t,k) \in \operatorname{dom} x$, we have $(t,k,y) \in K_e$; thus $G(y) \subset C \cup D$.

In order to prove the necessity part, we propose the barrier candidate $B : \mathbb{R}_{\geq 0} \times \mathbb{N} \times \mathbb{R}^n \to \mathbb{R}$ defined as

$$B(t,k,x) := \inf_{\begin{bmatrix} \phi \in \mathcal{S}^-(x) \\ -t \leq \tau \leq 0 \\ -k \leq j \leq 0 \\ (\tau, j) \in \operatorname{dom} \phi \end{bmatrix}} |\phi(\tau, j)|_{X_o}. \tag{34}$$

We recall that $\mathcal{S}^-(x)$, for $x \in C \cup D$, is the set of maximal backward solutions to $\mathcal{H}$ starting from x. When $x \in \mathbb{R}^n \backslash (C \cup D)$, $\mathcal{S}^-(x)$ reduces to the trivial function $x = x_o$ with $\operatorname{dom} x = \{(0,0)\}$ — see Section 2. Since the set X_o is closed, the system is safe, and each backward solution remains in a compact subset of $\mathbb{R}^n$ after any finite hybrid time, it follows that the backward solutions starting from $x \in X_u \cap (C \cup D)$ will neither reach nor converge to the set X_o after any finite hybrid time; hence, $B(t,k,x) > 0$ for all $(t,k,x) \in \mathbb{R}_{\geq 0} \times \mathbb{N} \times ((C \cup D) \cap X_u)$ which concludes (29). Furthermore, (28) is trivially satisfied under (34). Also, for each $x \in D$ reachable by a solution starting from X_o after a finite hybrid time (t,k), i.e. $(t,k,x) \in K_e$, each $\eta \in G(x) \neq \emptyset$ is also reachable by the same solution after the hybrid time $(t,k+1)$. Hence, using (34), condition (30) follows. Moreover, since the system is safe, $\eta \in C \cup D$; thus, (31) is also satisfied.

Next, we show that the barrier function B in (34) does not increase along the system's forward solutions flowing in C. Indeed, consider a solution $x : [t, t+h] \times \{k\} \to C$ flowing after the k-th

[3] By $\partial_p B(\cdot,k,\cdot)(t,x)$ we mean the proximal subdifferential computed at k with respect to the first and last components.

jump for some $h > 0$ such that $[t, t+h] \times \{k\} \subset \operatorname{dom} x$. That is,

$$\begin{aligned} B(t+h,k,x(t+h,k)) &= \inf_{\begin{bmatrix} \phi \in \mathcal{S}^-(x(t+h,k)) \\ -(t+h) \le \tau \le 0 \\ -k \le j \le 0 \\ (\tau, j) \in \operatorname{dom} \phi \end{bmatrix}} |\phi(\tau, j)|_{X_o} \\ &= \inf_{\begin{bmatrix} \phi \in \mathcal{S}(x(0,0)) \\ 0 \le \tau \le t+h \\ 0 \le j \le k \\ (\tau, j) \in \operatorname{dom} \phi \end{bmatrix}} |\phi(\tau, j)|_{X_o} \\ &\le \inf_{\begin{bmatrix} \phi \in \mathcal{S}(x(0,0)) \\ 0 \le \tau \le t \\ 0 \le j \le k \\ (\tau, j) \in \operatorname{dom} \phi \end{bmatrix}} |\phi(\tau, j)|_{X_o} \\ &= \inf_{\begin{bmatrix} \phi \in \mathcal{S}^-(x(t,k)) \\ -t \le \tau \le 0 \\ -k \le j \le 0 \\ (\tau, j) \in \operatorname{dom} \phi \end{bmatrix}} |\phi(\tau, j)|_{X_o} \\ &= B(t,k,x(t,k)). \end{aligned} \tag{35}$$

Hence, the barrier function B does not increase along the system's flows.

In the next step we show that $(t, x) \mapsto B(t, k, x)$ is lower semicontinuous using contradiction. Indeed, let us assume the existence of $(t_o, x_o) \in \mathbb{R}_{\ge 0} \times \mathbb{R}^n$ such that the barrier function B is not lower semicontinuous at (t_o, x_o). That is, there exists a sequence $\{(x_{io}, t_i)\}_{i=0}^{\infty}$ such that $(t_i, x_{io}) \in \mathbb{R}_{\ge 0} \times \mathbb{R}^n$, $\lim_{i\to\infty}(x_{io}, t_i) = (x_o, t_o)$, and

$$\begin{aligned} \lim_{i\to\infty} B(t_i,k,x_{io}) &= \lim_{i\to\infty} \inf_{\begin{bmatrix} \phi \in \mathcal{S}^-(x_{io}) \\ -t_i \le \tau \le 0 \\ -k \le j \le 0 \\ (\tau, j) \in \operatorname{dom} \phi \end{bmatrix}} |\phi(\tau, j)|_{X_o} \\ &< B(t_o,k,x_o). \end{aligned} \tag{36}$$

First, we notice the existence of a sequence of backward hybrid arcs $\{x_i\}_{i=0}^{\infty}$ such that, for all $i \ge 0$, $x_i \in \mathcal{S}^-(x_{io})$, $x_i : \operatorname{dom} x_i \to \mathbb{R}^n$, $x_i(0,0) = x_{io}$, and

$$\begin{aligned} B(t_i,k,x_{oi}) &= \inf_{\begin{bmatrix} \phi \in \mathcal{S}^-(x_{io}) \\ -t_i \le \tau \le 0 \\ -k \le j \le 0 \\ (\tau, j) \in \operatorname{dom} \phi \end{bmatrix}} |\phi(\tau, j)|_{X_o} \\ &= \inf_{\begin{bmatrix} -t_i \le \tau \le 0 \\ -k \le j \le 0 \\ (\tau, j) \in \operatorname{dom} x_i \end{bmatrix}} |x_i(\tau, j)|_{X_o}. \end{aligned} \tag{37}$$

Next, in order to use Lemma 2.1, we show that the sequence x_i is locally eventually bounded with respect to $\mathbb{R}^n$. The latter fact holds true using Lemma 2.2 under the assumption that the backward solutions do not escape in finite hybrid time inside the set $\mathbb{R}^n$. Hence, using Lemma 2.1, we conclude the existence of a subsequence $\{x_{i_l}\}_{l=0}^{\infty}$ that converges graphically to a backward hybrid arc $x \in \mathcal{S}^-(x_o)$ such that $x : \operatorname{dom} x \to \mathbb{R}^n$, $\operatorname{dom} x \subset [-t, 0] \times \{-k, \ldots, 0\}$, and $x(0,0) = x_o$. Moreover, for all $\epsilon > 0$ and for all $h > 0$ there exists $l_o \in \mathbb{N}$ such that for all $(\tau, j) \in \operatorname{dom} x_{i_l}$, $-t_{i_l} \le \tau \le 0$ and $j \le k$, there exists $s \in [0, t]$ such that $(s, j) \in \operatorname{dom} x$, $|\tau - s| < \epsilon$, and $|x(s, j) - x_{i_l}(\tau, j)| \le \epsilon$. The latter fact implies that

$$\begin{aligned} \lim_{l\to\infty} B(t_{i_l},k,x_{i_l o}) &= \lim_{l\to\infty} \inf_{\begin{bmatrix} \phi \in \mathcal{S}^-(x_{i_l o}) \\ -t_{i_l} \le \tau \le 0 \\ -k \le j \le 0 \\ (\tau, j) \in \operatorname{dom} \phi \end{bmatrix}} |\phi(\tau, j)|_{X_o} \\ &= \lim_{l\to\infty} \inf_{\begin{bmatrix} -t_{i_l} \le \tau \le 0 \\ -k \le j \le 0 \\ (\tau, j) \in \operatorname{dom} x_{i_l} \end{bmatrix}} |x_{i_l}(\tau, j)|_{X_o} \\ &= \inf_{\begin{bmatrix} -t_o \le \tau \le 0 \\ -k \le j \le 0 \\ (\tau, j) \in \operatorname{dom} x \end{bmatrix}} |x(\tau, j)|_{X_o} \\ &\ge \inf_{\begin{bmatrix} \phi \in \mathcal{S}^-(x_o) \\ -t_o \le \tau \le 0 \\ -k \le j \le 0 \\ (\tau, j) \in \operatorname{dom} \phi \end{bmatrix}} |\phi(\tau, j)|_{X_o} = B(t_o,k,x_o), \end{aligned}$$

where the last inequality follows from the definition of B in (34). Hence, a contradiction with (36) follows. Furthermore, since the lower semicontinuous barrier function B does not increase along the flows of $\mathcal{H}$, then it does not increase along any solution to the differential inclusion $\dot{x} \in F(x)$ lying in C. That is, if additionally (A7) holds and the flow map F is locally Lipschitz, using Lemma 2.4, (33) follows. □

Remark 5. For safe hybrid inclusions satisfying the assumptions of Theorem 3.4, the proposed barrier function certificate in (34) can only be lower semicontinuous in general. Indeed, even when both the flow and the jump maps are smooth and single valued, we can find examples where at some elements in the set $\partial(C \cap D)$, the barrier function in (34) is not lower semicontinuous, as shown next. •

Example 3. Consider the hybrid system with the following data:

$$F(x) := \begin{bmatrix} 1 & x_2 \end{bmatrix}^\top, \quad C := \left\{ x \in \mathbb{R}^2 : x_1 \ge 0 \right\},$$

$$G(x) := \begin{bmatrix} x_1 & -x_2 \end{bmatrix}^\top, \quad D := \left\{ x \in \mathbb{R}^2 : x_1 \le 0 \right\}.$$

It easy to see that conditions (A1)-(A4) are all satisfied. Furthermore,

$$G_D^{-1}(x) = \begin{bmatrix} x_1 & -x_2 \end{bmatrix}^\top = G(x)$$

for all $x \in G(D)$, and $G(D) = D$; hence, (A5)-(A6) are also satisfied. Consider the case where

$$X_o := \left\{ x \in \mathbb{R}^2 : x_1 \ge 0,\ x_2 = 0 \right\}, \quad X_u := \mathbb{R}^2 \setminus X_o.$$

In this particular case, it is easy to see that safety of the system with respect to (X_o, X_u) is equivalent to forward pre-invariance of the set X_o. Forward pre-invariance of X_o is satisfied since the solutions starting from X_o cannot leave this set neither after jumping nor after flowing. Then, Theorem 3.4 applies to conclude that the barrier function in (34) is a valid certificate for safety. However, we will show that such a barrier certificate is only lower semicontinuous and, in particular, fails to be continuous at elements of the set $\partial(C \cap D)$. For example, for $x_o = (0, 1)$ and $(t, k) \in \mathbb{R}_{>0} \times \mathbb{N}$, the sequence $\{x_{oi}\}_{i=0}^{\infty}$ with $x_{oi} := (-1/i, 1)$ satisfies $\lim_{i\to\infty} B(t,k,x_{oi}) \ne B(t,k,x_o)$. Indeed, $\lim_{i\to\infty} B(t,k,x_{oi}) = 1$ for all $i \in \mathbb{N}$ since the backward solution x_i starting from each x_{oi} is discrete and satisfies $|x_i(0,-k)|_{X_o} = |x_{oi}|$ for all $k \in \mathbb{N}$. Moreover, $B(t,k,x_o) = \exp(-t) \ne 1$ for all $t > 0$

since there exists a backward solution x flowing from x_o and satisfying $x(t,0) = (\exp(t), -t)$ for all $t \leq 0$. Thus, the candidate in (34) is not continuous. □

Remark 6. Assuming that the system's backward solutions are bounded or complete is important to show the existence of a lower semicontinuous barrier function for two reasons:

(1) When some backward solutions, starting from X_u, escape in finite time while converging to the set K, condition (29) will not be satisfied even if the system is safe — see Example 4.
(2) When the system's backward solutions are allowed to have a finite-time escape, the sequence of hybrid arcs used in the proof of Theorem 3.4 may fail to be locally eventually bounded, hence, graphical convergence of a subsequence could not be equivalent to the (T, J, ϵ)-closedness in Lemma 2.1. Thus, one cannot guarantee lower semicontinuity of the barrier function constructed in (34).

•

Example 4. To illustrate the first item in Remark 6, we consider the hybrid system with the following data:

$$F(x) := [-x_1^2 \quad x_1^2 x_2]^\top, \quad C := \left\{x \in \mathbb{R}^2 : x_1 \geq 0\right\},$$
$$G(x) := [x_1 \quad -x_2]^\top, \quad D := \left\{x \in \mathbb{R}^2 : x_1 \leq 0\right\}.$$

Conditions (A1)-(A4) are verified,

$$G_D^{-1}(x) = [x_1 \quad -x_2]^\top = G(x)$$

for all $x \in G(D)$, and $G(D) = D$; hence, (A5)-(A6) are also verified. However, the system's backward solutions starting from $x_1 > 0$ escape in finite time. As a consequence, we shall show that the barrier candidate proposed in (34) does not satisfy condition (29) for a particular choice of (X_o, X_u) such that the system is safe. Thus, the latter barrier candidate is not a valid certificate according to Theorem 3.4 for this particular example. As in Example 3, consider the case where

$$X_o := \left\{x \in \mathbb{R}^2 : x_1 \geq 0,\ x_2 = 0\right\}, \quad X_u := \mathbb{R}^2 \setminus X_o.$$

Forward pre-invariance of the set X_o is satisfied, hence, the safety property is verified. Furthermore, consider the system's backward solution flowing from $x_o = (1,1)$. The analytic expression of such a solution is given by $x(t) = (1/(1+t), \exp(-x_1(t)))$ for all $t \leq 0$. It is easy to see that when $t \to -1$, x converges to the set X_o while escaping the horizon. Hence, $B(1,0,x_o) = 0$ even if $x_o \in X_u$. The later fact implies that condition (29) is not satisfied. □

Next, we propose a concrete example of a hybrid system that satisfies the assumptions in Theorem 3.4.

Example 5. Theorem 3.4 applies for the dynamical hybrid system model of a bouncing ball. This system has the following data:

$$F(x) := [x_2 \quad -\gamma]^\top, \quad C := \left\{x \in \mathbb{R}^2 : x_1 \geq 0\right\},$$
$$G(x) := [0 \quad -\lambda x_2]^\top, \quad D := \left\{x \in \mathbb{R}^2 : x_1 = 0,\ x_2 \leq 0\right\}.$$

The constants $\gamma > 0$ and $\lambda \in [0,1]$ are the gravity acceleration and the restitution coefficient, respectively. Conditions (A1)-(A4) are satisfied, and the flow map F is smooth and locally Lipschitz. Furthermore, $G_D^{-1}(x) := [0 \quad \lambda x_2]^\top$ for all $x \in G(D)$, and

$$G(D) := \left\{x \in \mathbb{R}^2 : x_1 = 0,\ x_2 \geq 0\right\};$$

hence, (A5)-(A6) are also satisfied. Finally, (A7) is satisfied only when ∂C therein replaced by $(\partial C) \setminus \{(0,0)\}$. Indeed, F is single valued and continuous, and $F(x) \in T_C(x)$ for all $x \in \partial C \setminus D$.

As a consequence, given any closed set of initial conditions X_o and unsafe set X_u, the bouncing ball model is safe with respect to a given (X_o, X_u) if and only if there exists a (hybrid) time-varying lower semicontinuous and nonincreasing along the flows barrier function $B : \mathbb{R}_{\geq 0} \times \mathbb{N} \times \mathbb{R}^2$ such that (28)-(31) hold. Moreover, when safety holds, the inequality in (33) also holds for all $(t,k,x) \in \mathbb{R}_{\geq 0} \times \mathbb{N} \times (C \setminus D)$. □

A direct consequence of Theorem 3.4 concerns the particular cases of a pure differential inclusion ($\mathcal{H} = \mathcal{H}_f := (\mathbb{R}^n, F, \emptyset, 0)$) or of a pure difference inclusion ($\mathcal{H} = \mathcal{H}_d := (\emptyset, 0, \mathbb{R}^n, G)$). Safety in such situations is characterized next using barrier functions.

Corollary 1. *Given a differential inclusion $\mathcal{H}_f := (\mathbb{R}^n, F, \emptyset, 0)$, assume that (A1)-(A2) holds and F locally Lipschitz. Let the set X_o be closed and suppose that every maximal backward solution is bounded or complete. Then, the system $\mathcal{H}_f$ is safe with respect to (X_o, X_u) if and only if there exists a barrier function $B : \mathbb{R}_{\geq 0} \times \mathbb{R}^n \to \mathbb{R}$ such that $(t,x) \mapsto B(t,x)$ is lower semicontinuous, and*

$$B(t,x) \leq 0 \qquad \forall (t,x) \in \mathbb{R}_{\geq 0} \times X_o, \tag{38}$$
$$B(t,x) > 0 \qquad \forall (t,x) \in \mathbb{R}_{\geq 0} \times X_u, \tag{39}$$
$$\theta + \langle \zeta, \eta \rangle \leq 0 \qquad \forall \eta \in F(x),\ \forall (\theta, \zeta) \in \partial_P B(t,x),\ \text{and } \forall (t,x) \in \mathbb{R}_{\geq 0} \times \mathbb{R}^n. \tag{40}$$

□

Corollary 2. *Given the difference inclusion $\mathcal{H}_j := (\emptyset, 0, \mathbb{R}^n, G)$, assume that (A3)-(A6) hold. Let the set X_o be closed. Then, the system $\mathcal{H}_d$ is safe with respect to (X_o, X_u) if and only if there exists a barrier function $B : \mathbb{N} \times \mathbb{R}^n \to \mathbb{R}$ such that $x \mapsto B(k,x)$ is lower semicontinuous, and*

$$B(k,x) \leq 0 \qquad \forall (k,x) \in \mathbb{N} \times X_o, \tag{41}$$
$$B(k,x) > 0 \qquad \forall (k,x) \in \mathbb{N} \times X_u, \tag{42}$$
$$B(k+1,\eta) \leq 0 \qquad \forall \eta \in G(x), \quad \forall (k,x) \in (\mathbb{N} \times \mathbb{R}^n) \cap K_e, \tag{43}$$
$$\text{where} \quad K_e := \left\{(k,x) \in \mathbb{N} \times \mathbb{R}^n : B(k,x) \leq 0\right\}. \tag{44}$$

□

3.4 Necessary and sufficient conditions for particular cases

3.4.1 ***Compact initial set.*** The following result extends the statement of Theorem 3.4 when the initial set X_o is bounded. In this case, the statement of Theorem 3.4 remains true even if the system's backward solutions escape in finite time.

Theorem 3.5. *Given a hybrid system $\mathcal{H}$, assume that (A1)-(A6) hold. Let the set X_o be compact. Then, the system $\mathcal{H}$ is safe with respect to (X_o, X_u) if and only if there exists a barrier function $B : \mathbb{R}_{\geq 0} \times \mathbb{N} \times \mathbb{R}^n \to \mathbb{R}$ such that, uniformly in k, $(t,x) \mapsto B(t,k,x)$ is lower semicontinuous, nonincreasing along the flows and* (28)-(31) *hold. Moreover, if additionally (A7) holds and the flow map F is locally Lipschitz,* (33) *holds.*

Sketch of proof: The sufficient part of the statement can be proved using the same steps as in the proof of Theorem 3.4. In order to prove the necessary part, we adapt the steps in the proof of Theorem 3.4 to the current statement. We also consider the barrier candidate $B : \mathbb{R}_{\geq 0} \times \mathbb{N} \times \mathbb{R}^n \to \mathbb{R}$ introduced in (34). Then, (28)-(31), and the fact that the barrier function B in (34) does not increase along the system's forward flows lying in C follow using the same arguments as in the proof of Theorem 3.4. Next, in order to show that

$(t, x_o) \mapsto B(t, k, x_o)$ is lower semicontinuous even if the system's backward solutions can escape in finite time, we use the compactness of the set X_o. Indeed, since the set X_o is compact, whenever a backward solution x escapes in finite time, it will reach its minimum distance with respect to the set X_o before the escape time. Hence, the backward solution x starting from x_o can be restricted to the domain $[0, T_x] \times \{1, \ldots, J_x\}$ for some $T_x \geq 0$ and $J_x \in \mathbb{N}$. Such a restriction is contained in a compact subset of the studied space and it cannot have a finite-time escape. In this way, we define the backward truncation $\hat{x}$ for all $x \in \mathcal{S}^-(x_o)$ as

$$\hat{x} := \begin{cases} x & \text{if } x \text{ does not escape in finite time,} \\ x \text{ restricted to } [0, T_x] \times \{1, \ldots, J_x\} & \text{otherwise.} \end{cases}$$

Then, define $\hat{\mathcal{S}}^-(x_o)$ as the set of all the truncations starting from x_o. Hence,

$$B(t,k,x_o) = \inf_{\begin{bmatrix} x \in \mathcal{S}^-(x_o) \\ -t \leq \tau \leq 0 \\ -k \leq j \leq 0 \\ (\tau, j) \in \operatorname{dom} x \end{bmatrix}} |x(\tau, j)|_{X_o} = \inf_{\begin{bmatrix} \hat{x} \in \hat{\mathcal{S}}^-(x_o) \\ -t \leq \tau \leq 0 \\ -k \leq j \leq 0 \\ (\tau, j) \in \operatorname{dom} \hat{x} \end{bmatrix}} |\hat{x}(\tau, j)|_{X_o}.$$

With this property, the reminder of the proof uses the same arguments used in the proof of Theorem 3.4. Finally, if additionally (A7) holds and the flow map F is locally Lipschitz, (33) follows using Lemma 2.4. ■

3.4.2 ***Non-Zeno backward solutions.*** The following result extends Theorem 3.4 when the system's backward solutions are non-Zeno.

Theorem 3.6. *Given a hybrid system $\mathcal{H}$ such that the assumptions in Theorem 3.4 hold. Assume that the system's backward solutions are non-Zeno. Then, the system $\mathcal{H}$ is safe with respect to (X_o, X_u) if and only if there exists a lower semicontinuous barrier function $B : \mathbb{R}_{\geq 0} \times \mathbb{R}^n \to \mathbb{R}$ such that B does not increase along the flows of $\mathcal{H}$ and the following conditions hold:*

$$B(t, x) \leq 0 \qquad \forall (t, x) \in \mathbb{R}_{\geq 0} \times X_o, \tag{45}$$

$$B(t, x) > 0 \qquad \forall (t, x) \in \mathbb{R}_{\geq 0} \times (X_u \cap (C \cup D)), \tag{46}$$

$$B(t, \eta) \leq 0 \qquad \forall \eta \in G(x) \quad \forall (t, x) \in K_e \cap (\mathbb{R}_{\geq 0} \times D), \tag{47}$$

$$G(x) \subset C \cup D \qquad \forall x \in D \text{ s.t. } (t, x) \in K_e \text{ for some } t \geq 0, \tag{48}$$

$$\text{where} \quad K_e := \left\{(t, x) \in \mathbb{R}_{\geq 0} \times \mathbb{R}^n : B(t, x) \leq 0\right\}. \tag{49}$$

Moreover, if (A7) holds and the flow map F is locally Lipschitz, the barrier B satisfies

$$\theta + \langle \zeta, \eta \rangle \leq 0 \qquad \forall \eta \in F(x) \cap T_C(x),\ \forall (\theta, \zeta) \in \partial_P B(t, x), \quad \text{and } \forall (t, x) \in \mathbb{R}_{\geq 0} \times C. \tag{50}$$

Sketch of proof: The proof of the sufficient part is the same as in the proof of Theorem 3.4. To prove the necessity part, we introduce the barrier candidate $B : \mathbb{R}_{\geq 0} \times \mathbb{R}^n \to \mathbb{R}$ as

$$B(t, x) := \inf_{\begin{bmatrix} \phi \in \mathcal{S}^-(x) \\ -t \leq \tau \leq 0 \\ -\kappa(t, \phi) \leq j \leq 0 \\ (\tau, j) \in \operatorname{dom} \phi \end{bmatrix}} |\phi(\tau, j, x)|_{X_o}, \tag{51}$$

where $\kappa : \mathbb{R}_{\geq 0} \times \mathcal{S}^-(x) \to \mathbb{N}$ determines the number of jumps in the backward hybrid arc ϕ in the interval $[-t, 0]$. The function κ is well-defined since the system's solutions are non-Zeno. Furthermore, under (34), one can show that the conditions (45)-(48) are satisfied and the barrier function B does not increase along the system's flows using the same arguments in the proof of Theorem 3.4. Also, in order to show that $(t, x) \mapsto B(t, x)$ is lower semicontinuous, the same arguments in the proof of Theorem 3.4 can be used in combination with the fact that, for a locally eventually bounded and graphically convergent sequence of hybrid arcs, the corresponding sequence of hybrid time domains converges graphically to a hybrid time domain, which is the domain of the sequence's graphical limit, see [19, Theorem 4.26] and [5, Example 5.19]. Furthermore, since the lower semicontinuous barrier function B does not increase along the flows of $\mathcal{H}$, if additionally (A7) holds and the flow map F is locally Lipschitz, (50) follows using Lemma 2.4. ■

4 CONCLUSION

In this study we proposed necessary and sufficient conditions guaranteeing safety in terms of barrier functions for general hybrid inclusions. In particular, characterizations involving continuously differentiable as well as lower semicontinuous barrier functions are proposed. Furthermore, inspired by converse Lyapunov theorems for only stability, safety is shown to be equivalent to the existence of a nonautonomous lower semicontinuous barrier function satisfying sufficient conditions for safety, under mild regularity conditions on the data of the hybrid inclusion.

REFERENCES

[1] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada. 2017. Control barrier function based quadratic programs for safety critical systems. *IEEE Trans. Automat. Control* 62, 8 (2017), 3861–3876.
[2] J. P. Aubin and H. Frankowska. 2009. *Set-valued analysis.* Springer Science & Business Media.
[3] D. Belleter, M. Maghenem, C. Paliotta, and K. Y. Pettersen. 2019. Observer based path following for underactuated marine vessels in the presence of ocean currents: A global approach. *Automatica* 100 (2019), 123 – 134. https://doi.org/10.1016/j.automatica.2018.11.008
[4] F. H. Clarke, Y. S. Ledyaev, R. J. Stern, and P. R. Wolenski. 2008. *Nonsmooth analysis and control theory.* Vol. 178. Springer Science & Business Media.
[5] R. Goebel, R. G. Sanfelice, and A. R. Teel. 2012. *Hybrid Dynamical Systems: modeling, stability, and robustness.* Princeton University Press.
[6] R. Goebel and A. R. Teel. 2006. Solutions to hybrid inclusions via set and graphical convergence with stability theory applications. *Automatica* 42, 4 (2006), 573–587.
[7] W. Hahn. 1967. *Stability of motion.* Vol. 138. Springer.
[8] A. A. Kayande and V. Lakshmikantham. 1966. Conditionally invariant sets and vector Lyapunov functions. *J. Math. Anal. Appl.* 14, 2 (1966), 285–293.
[9] N. N. Krasovskii. 1963. *Stability of Motion. Applications of Lyapunov's second method to differential systems and equations with delay. Translated by J. L. Brenner.* Vol. 48s. Standford University Press.
[10] J. Kurzweil. 1955. On the inversion of Lyapunov's first theorem on the stability of motion (In Russian). *Czechoslovak Mathematical Journal* 5, 3 (1955), 382–398.
[11] J. Kurzweil and I. Vrkoč. 1957. Transformation of Lyapunov's theorems on stability and Persidskii's theorems on uniform stability (In Russian). *Czechoslovak Mathematical Journal* 7, 2 (1957), 254–272.
[12] G. S. Ladde and V. Lakshmikantham. 1974. On flow-invariant sets. *Pacific J. Math.* 51, 1 (1974), 215–220.
[13] M. Maghenem and R. G. Sanfelice. 2019. On the characterization of safety and conditional invariance in dynamical systems. (2019). To appear in 2019 American Control Conference.
[14] E. Michael. 1956. Continuous selections. I. *Annals of mathematics* (1956), 361–382.
[15] K. P. Persidskii. 1937. On a theorem of Liapunov. *C. R. (Dokl.) Acad. Sci. URSS* 14 (1937), 541–543.
[16] S. Prajna. 2005. *Optimization-based methods for nonlinear and hybrid systems verification.* Ph.D. Dissertation. California Institute of Technology.
[17] S. Prajna, A. Jadbabaie, and G. J. Pappas. 2007. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Trans. Automat. Control* 52, 8 (2007), 1415–1428.
[18] S. Prajna and A. Rantzer. 2005. On the necessity of barrier certificates. *IFAC Proceedings Volumes* 38, 1 (2005), 526–531.
[19] R. T. Rockafellar and J. B. R Wets. 1997. *Variational analysis.* Vol. 317. Springer Science & Business Media.
[20] A. Taly and A. Tiwari. 2009. Deductive verification of continuous dynamical systems. In *LIPIcs-Leibniz International Proceedings in Informatics*, Vol. 4. Schloss Dagstuhl-Leibniz-Zentrum für Informatik.
[21] H. G. Tanner, A. Jadbabaie, and G. J. Pappas. 2003. Stable flocking of mobile agents, Part I: Fixed topology, Vol. 2. IEEE, 2010–2015.

[22] K. P. Tee, S. S. Ge, and E. H. Tay. 2009. Barrier Lyapunov functions for the control of output-constrained nonlinear systems. *Automatica* 45, 4 (2009), 918–927.
[23] P. Wieland and F. Allgöwer. 2007. Constructive safety using control barrier functions. *IFAC Proceedings Volumes* 40, 12 (2007), 462–467.
[24] A. G. Wills and W. P. Heath. 2004. Barrier function based model predictive control. *Automatica* 40, 8 (2004), 1415 – 1422.
[25] R. Wisniewski and C. Sloth. 2016. Converse barrier certificate theorems. *IEEE Trans. Automat. Control* 61, 5 (2016), 1356–1361.