2019 American Control Conference (ACC)
Philadelphia, PA, USA, July 10-12, 2019

Characterization of Safety and Conditional Invariance for Nonlinear Systems

Mohamed Maghenem and Ricardo G. Sanfelice

Abstract— **This paper investigates sufficient and necessary conditions for safety (equivalently, conditional invariance) in terms of barrier functions. Relaxed sufficient conditions concerning the sign and the regularity of the barrier function are proposed. Furthermore, via a counterexample, the lack of existence of an autonomous and continuous barrier function certifying safety in a class of autonomous systems is shown. As a consequence, guided by converse Lyapunov theorems for only stability, time-varying barrier functions are proposed and infinitesimal conditions are shown to be both necessary as well as sufficient, provided that mild regularity conditions on the system's dynamics holds. Examples illustrate the results.**

I. INTRODUCTION

Beyond stability, the most important property to guarantee in a dynamical system is safety. The safety problem consists in guaranteeing that the system's solutions, when starting from a given *set of initial conditions*, never reach a given *unsafe set* [1]. The same property is also called *conditional invariance* in some earlier works [2], [3], [4], [5]. Regarding the considered application, reaching the unsafe set can correspond to the impossibility of applying a predefined feedback law [6] or, simply, colliding with an obstacle [7]. Safety analysis is in fact a key step in many control applications.

Analogous to Lyapunov theory for stability, the concept of barrier function is a powerful qualitative tool to study safety without computing the system's solutions. Generally speaking, a barrier function candidate is a function of the system's variables that satisfies some sign and boundedness properties on the set of initial conditions and the opposite properties around the unsafe set. Then, the safety property is guaranteed provided that the change of the barrier candidate along the system's solutions, which can written in terms of infinitesimal conditions, satisfies certain growth conditions, especially around the unsafe set. Hence, the barrier candidate becomes a safety certificate in this case. According to the latter definition, barrier functions are used in many contexts including constrained optimization [8], multiagent systems [7], and constrained nonlinear control [9], to just name a few. Furthermore, barrier functions have been used under different names in the literature, including *potential* functions [7] and even just *Lyapunov* functions in some earlier works [5]. Also, barrier functions adopt different forms in the literature. For example, in [10], a barrier function candidate is defined as a positive function that is is bounded on the set of initial conditions and unbounded when converging to the boundary of the unsafe set. In [1] and [11], a barrier function candidate is defined as a scalar function that is strictly positive on the unsafe set and nonpositive on the set of initial conditions. Another slightly different definition can be deduced from [2], where a barrier function candidate is assumed to have values on the boundary of the unsafe set strictly greater than on the boundary of the initial set.

In the context of safety analysis using barrier functions, as compared to Lyapunov theory for stability, the converse problem is less explored and not completely solved. 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 such that a barrier function verifying sufficient conditions for safety exists. For sufficiently smooth systems and when a continuously differentiable and strictly decreasing function along the system's solutions exists, it is shown in [12] that safety is equivalent to the existence of a smooth barrier function. In [13], after reintroducing the notion of safety, a converse result is proposed for smooth systems living in smooth compact manifolds. In this case, the latter assumption in [12] is replaced by the existence of certain type of functions known as *Meyer* functions. In [13], it is also pointed out that the assumption in [12] is restrictive as it excludes, for example, systems with limit cycles. Furthermore, when the set of initial conditions or the unsafe set are not compact, the converse result in [13] does not apply — see Example 1 in this paper. To the best of our knowledge, [12] and [13] are the only works on converse characterizations of safety using barrier functions.

In this paper, we compare and relax some of the existing sufficient conditions for safety using barrier functions. The proposed relaxations concern the sign and the regularity of the barrier candidates. After that, we propose to study the necessity of the proposed sufficient conditions. We present a simple yet informative counter-example that shows that, in some situations, it is not possible to construct a continuous barrier function depending only on the system's variables such that the proposed sufficient conditions hold. This is true even when the system is smooth and autonomous. Consequently, we propose time-varying barrier functions and sufficient conditions for safety that are also necessary, under

M. Maghenem and R. G. Sanfelice are with Department of Electrical and Computer Engineering, University of California, Santa Cruz. Email: mmaghene,ricardo@ucsc.edu.

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.

978-1-5386-7926-5/$31.00 ©2019 AACC

mild regularities on the system's dynamics. The latter is not to be confused with the time-varying barrier functions used in the context of moving obstacles [14] and providing only sufficient conditions for safety. Our approach is inspired from converse Lyapunov theorems for only stability in [15], [16], [17], [18], [19]. To the best of our knowledge, the proposed results are unique in the literature and open the field to having general converse characterizations for safety using barrier functions.

The reminder of the paper is organized as follows. Background and motivations are presented in Section II. Sufficient conditions for safety in terms of barrier functions are in Section III, and necessary and sufficient conditions in terms of barrier functions are in Section IV.

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

Notation. For $x,\ y \in \mathbb{R}^n$, $x^\top$ denotes the transpose of x, $|x|$ the Euclidean norm of x, $|x|_K := \inf_{y\in K} |x-y|$ defines the distance between x and the set K, and $\langle x, y\rangle$ denotes 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 $U(K)$ an open neighborhood around K. For $O \subset \mathbb{R}^n$, $K\backslash O$ denotes the subset of elements of K that are not in O. For a function $f : \mathbb{R}^n \to \mathbb{R}^m$, $\text{dom}\, f$ denotes the domain of definition of f, $f^{-1}(x)$ denotes its reciprocal image evaluated at x. Finally, by $f \in \mathcal{C}^k(K)$, $k \in \{1, 2, ..\}$, we mean that f is $k-$times differentiable and the $k-$th derivative is continuous (when $K = \mathbb{R}^n$, we only write $f \in \mathcal{C}^k$).

II. Background and Motivation

A. Background on safety problem

Consider a differential equation of the form

$$\dot{x} = f(x) \tag{1}$$

where $f : \mathbb{R}^n \to \mathbb{R}^n$. A solution $x : \text{dom}\, x \to \mathbb{R}^n$ to (1), starting from x_o, is given by a function $t \mapsto x(t, x_o)$ satisfying (1) for all $t \in \text{dom}\, x$, where $\text{dom}\, x \subset \mathbb{R}_{\geq 0}$ denotes the domain of definition of the solution x. A solution x is complete if $\text{dom}\, x$ is unbounded, and it is maximal if there is no solution y such that $y(t) = x(t)$ for all $t \in \text{dom}\, x$ and $\text{dom}\, x$ strictly included in $\text{dom}\, y$.

Results to study safety for such dynamical systems have been presented in [20], [11], [1], [12], [13]. In these articles, a set $X_u \subset \mathbb{R}^n$ denotes the region of the state space that the solutions to (1) are not allowed to reach when starting from a given set of initial conditions $X_o \subset \mathbb{R}^n\backslash X_u$.

Definition 1 (Safety): The system (1) is said to be safe with respect to (X_o, X_u), with $X_o \subset \mathbb{R}^n\backslash X_u$, if for each $x_o \in X_o$ and each solution x, $x(t, x_o) \in \mathbb{R}^n\backslash X_u$ for all $t \in \text{dom}\, x$. •

This definition of safety coincides with the definition of conditional invariance established in earlier literature; see [2], [3], [4], [5]. For completeness and comparison to safety as in Definition 1, we include the definition of conditional invariance, directly from [2].

Definition 2 (Conditional invariance): A set $H \subset \mathbb{R}^n$ is said to be conditionally invariant for (1) with respect to a set $F \subset H$ if, for each $x_o \in F$, each solution x starting from x_o satisfies $x(t, x_o) \in H$ for all $t \in \text{dom}\, x$. •

It is immediate that the system (1) is safe with respect to (X_o, X_u) if and only if the set $H := \mathbb{R}^n\backslash X_u$ is conditionally invariant for (1) with respect to $F := X_o$.

In what follows we recall existing sufficient conditions for safety from [1] and conditional invariance from [2]. Furthermore, we emphasize that the characterization in [2] allows a larger family of barrier functions in the case of continuous-time systems than the one in [1]. In [1], safety of (1) with respect to (X_o, X_u) is guaranteed by the existence of a $\mathcal{C}^1$ function $B : \mathbb{R}^n \to \mathbb{R}$ satisfying

$$\begin{cases} B(x) > 0 & \forall x \in X_u \\ B(x) \leq 0 & \forall x \in X_o \\ \langle \nabla B(x), f(x)\rangle \leq 0 & \forall x \in \mathbb{R}^n. \end{cases} \tag{2}$$

Such a function is called a barrier function in [1]. Conditions in (2) inform us not only about the safety with respect to (X_o, X_u), but more precisely about the forward invariance of the set

$$K := \{x \in \mathbb{R}^n : B(x) \leq 0\}. \tag{3}$$

On the other hand, following the earlier result in [2], the conditional invariance of a set H with respect to a set $F \subset H$ is guaranteed by the existence of a $\mathcal{C}^1$ function $\bar{B} : \mathbb{R}^n \to \mathbb{R}$ such that the following three conditions hold:

(i) For all $x \in \mathbb{R}^n\backslash F$ and all $y \in F$ such that

$$y = \arg\min_{z\in F} \bar{B}(x - z), \tag{4}$$

we have

$$\langle \nabla \bar{B}(x - y), f(y)\rangle \leq 0.$$

(ii) Define

$$w(x) := \bar{B}(x - y),$$

with y satisfying (4). Then, there exists $a \in \mathbb{R}$ such that

$$\begin{cases} w(x) \geq a & \forall x \in \partial H \\ w(x) < a & \forall x \in \partial F \end{cases} \tag{5}$$

(iii) For all $(x, y) \in (\mathbb{R}^n\backslash F) \times F$,

$$\dot{\bar{B}}(x - y) \leq g(\bar{B}(x - y)); \tag{6}$$

where the scalar function g is such that, for any $l : \mathbb{R}_{\geq 0} \to \mathbb{R}$, if $l(0) < a$ with a as in (ii) and

$$\begin{aligned} D^+ l(t) :=& \limsup_{t\to 0^+} \frac{l(t+h) - l(t)}{h} \\ &\leq g(l(t)) \qquad \forall t \geq 0, \end{aligned}$$

then, for some $\epsilon > 0$, $l(t) < a$ for all $t \in [0, \epsilon]$.

In [2], the main idea to proof conditional invariance for (1) of H with respect to F uses (5), which establishes that the value of w on the boundary of H is strictly larger than its value on the boundary of F. Then, using (i)-(iii), one can show that w does not increase along the solutions to (1). The latter fact is true since, under (i)-(iii), for each solution $t \mapsto x(t, x_o)$, we have

$$D^+ w(x(t, x_o)) \leq g(w(x(t, x_o))) \quad \forall t \in \operatorname{dom} x. \tag{7}$$

Hence, for any $x_o \in \partial F$, $w(x(t, x_o)) < a$ for all $t \in \operatorname{dom} x$. Consequently, there is not a possibility that a solution to (1), starting from F, reaches H.

Remark 1: Conditions (i)-(iii) guarantee forward invariance of the set

$$K_1 := \{x \in \mathbb{R}^n : w(x) - a < 0\},$$

which implies forward invariance of the set $K := (K_1 \cup F) \cap H$. Indeed, when a solution x to (1) starts from $K_1 \cap H$, it remains in $K_1 \cap H$ because of (7) and the fact that $w(x) \geq a$ for all $x \in \partial H$. Moreover, when a solution starts from F, it cannot leave the set F without flowing in $K_1 \cap H$ since $\partial F \subset K_1 \cap H$; hence, it also remains in K. •

Remark 2: We stress on the fact that conditions (i)-(iii) show that $\operatorname{int}(H)$ is conditionally invariant with respect to F. We implicitly assumed in this case that $F \subset \operatorname{int}(H)$. In the sequel, when $\operatorname{int}(H)$ is conditionally invariant with respect to F we say that H is *strictly conditionally invariant* with respect to F. The conditional invariance of H with respect to F holds if we replace condition (ii) by

(iv) Define $w(x) := \inf_{y \in F} \bar{B}(x - y)$, where x and y are as in (i), and there exists $a \in \mathbb{R}$ such that

$$w(x) > a \qquad \forall x \in U(H) \backslash H, \tag{8}$$

$$w(x) \leq a \qquad \forall x \in \partial F. \tag{9}$$

In this case, we are implicitly showing forward invariance of the set

$$K_2 := \{x \in H : w(x) - a \leq 0\} \cup F.$$

•

B. Background on converse safety problem

In [12], when additionally the vector field f is $\mathcal{C}^1$ and there exists a $\mathcal{C}^1$ function $g : \mathbb{R}^n \to \mathbb{R}$ that is strictly decreasing along the solutions to (1), it is shown that safety with respect to (X_o, X_u) implies the existence of a $\mathcal{C}^1$ barrier candidate B satisfying (2). Similarly, in [13], a geometric point of view is adopted using *Morse-Smale* theory for systems on smooth and compact manifolds. In this study, a slightly different definition of safety is considered and a converse result is proposed for such particular class of systems. The assumption about existence of a strictly decreasing function along the system's solutions in [12] is replaced in [13] by the existence of certain type of functions called *Meyer* functions.

C. Motivation

The contributions of this paper are two-fold:

- We investigate the tightest possible sufficient conditions for conditional invariance (equivalently, safety) in continuous-time systems.
- We provide necessary and sufficient conditions without assuming the existence of neither a strictly decreasing function along the solutions to (1) nor a *Meyer* function.

The relevance of our approach is justified in the following example.

Example 1: Consider the linear system

$$\dot{x}_1 = -10 x_2, \qquad \dot{x}_2 = x_1. \tag{10}$$

We analyze conditional invariance of the set

$$H := \left\{x \in \mathbb{R}^2 : x_2 \leq 2\right\}$$

with respect to the set

$$F := \left\{x \in \mathbb{R}^2 : x_1^2 + x_2^2 \leq 1\right\}.$$

First, note that neither F nor H are forward invariant. However, H is conditionally invariant for (10) with respect to F. A way to show this fact is to use the sufficient conditions in (2). For this purpose, we propose the barrier function candidate

$$B(x) := (x_1^2/10 + x_2^2) - 1. \tag{11}$$

The conditions in (2) are satisfied since $B(x) \leq 0$ for all $x \in X_o := F$, $B(x) > 0$ for all $x \in X_u := \mathbb{R}^n \backslash F$, and $\langle \nabla B(x), f(x) \rangle \leq 0$ for all $x \in \mathbb{R}^2$ and where $f(x) := [-10x_2 \quad x_1]^\top$. Hence, safety with respect to (X_o, X_u) follows. Thus, H is conditionally invariant with respect to F.

Another way to show this fact is inspired by conditions (i)-(iii) and the scalar function

$$\delta(x) := 10x_2^2 + x_1^2 - 1 \qquad \forall x \in \mathbb{R}^2. \tag{12}$$

We notice that

$$\langle \nabla \delta(x), f(x) \rangle = 0 \qquad \forall x \in \mathbb{R}^2, \tag{13}$$

and at the same time,

$$\sup_{x \in \partial F} \delta(x) = 9, \qquad \inf_{x \in \partial H} \delta(x) > 36. \tag{14}$$

Hence,

$$\delta(x) - \delta(y) < 0 \quad \forall x \in \partial F, \ \forall y \in \partial H. \tag{15}$$

Conditions (13) and (15) imply conditional invariance since if there was a solution x to (10) that evolves from a point in ∂F to ∂H, the value of δ would grow from $\delta(x(0)) \leq 9$ to $\delta(x(T)) \geq 36$ for some $T > 0$, which contradicts (13). Hence, solutions starting from the set F have to remain in the interior of the set H. It is important to notice that the family of barrier functions satisfying (13) and (15) is larger than the family of those satisfying (2).

Even though it was not very hard to find a barrier candidate satisfying (2), the existing converse results in [12] and [13] do not guarantee the existence of such a function for system (10), though it is safe. Indeed, it is not possible to find a function that is strictly decreasing along the system's solutions since the system admits limit cycles. Also, the set $X_u = \mathbb{R}^2 \backslash H$ is not bounded, hence, it is not a compact manifold. □

III. Sufficient Conditions for Safety

In this section we propose tight sufficient conditions in terms of the sign and the regularity of the barrier candidates. To cover the existing results in the literature, we consider two types of conditional invariance, namely, *strict conditional invariance* where the solutions starting from F remain in the interior of H, and *conditional invariance* where the solutions starting from F remain in H.

Theorem 1: Consider the differential equation in (1) with $f \in \mathcal{C}^o$. The following hold:

- A set $H \subset \mathbb{R}^n$ is conditionally invariant with respect to $F \subset H$ if there exists a function[1] $\delta \in \mathcal{C}^o \cap \mathcal{C}^1(U(H)\backslash F)$ such that

$$\begin{aligned} \langle \nabla \delta(x), f(x) \rangle &\leq 0 \quad \forall x \in U(H)\backslash F, & (16)\\ \delta(x) - \delta(y) &< 0 \quad \forall (x,y) \in \partial F \times (U(H)\backslash H). & (17) \end{aligned}$$

- A set H is strictly conditionally invariant with respect to $F \subset \text{int}(H)$ if there exists a function $\delta \in \mathcal{C}^o \cap \mathcal{C}^1(H\backslash F)$ such that

$$\begin{aligned} \langle \nabla \delta(x), f(x) \rangle &\leq 0 \qquad \forall x \in H\backslash F, & (18)\\ \delta(x) - \delta(y) &< 0 \qquad \forall (x,y) \in \partial F \times \partial H. & (19) \end{aligned}$$

□

In the following corollary, as a particular case of Theorem 1, we relax the sufficient conditions for safety in (2) by considering barrier functions $B : \mathbb{R}^n \to \mathbb{R}$ of class $\mathcal{C}^1$ only outside the set

$$K := \{x \in \mathbb{R}^n : B(x) \leq 0\} \quad (20)$$

and not necessarily on the entire state space.

Corollary 1: The system (1) with $f \in \mathcal{C}^o$ is safe with respect to given sets (X_o, X_u) if there exists a function $B \in \mathcal{C}^o \cap \mathcal{C}^1(\mathbb{R}^n \backslash K)$ such that

$$\begin{cases} B(x) > 0 & \forall x \in X_u, \\ B(x) \leq 0 & \forall x \in X_o, \\ \langle \nabla B(x), f(x) \rangle \leq 0 & \forall x \in \mathbb{R}^n \backslash K. \end{cases} \quad (21)$$

□

When the function δ used in Theorem 1 is only locally Lipschitz, we replace the monotonicity condition (16) (respectively, (18)) by a similar one using the *proximal subdifferential* instead of the gradient. In general, for a lower semicontinuous function $\delta : \mathbb{R}^n \to \mathbb{R}$, we use $\partial_P \delta(x)$ to denote its *proximal subdifferential* evaluated at x, which can be defined as

$$\begin{aligned} \partial_P \delta(x) := \{\zeta \in \mathbb{R}^n : \exists U(x),\ \exists \epsilon > 0 : \forall y \in U(x) \\ \delta(y) \geq \delta(x) + \langle \zeta, y - x \rangle - \epsilon |y - x|^2 \}. \quad (22) \end{aligned}$$

Each vector $\zeta \in \partial_P \delta(x)$ is said to be a *proximal subgradient* of δ at x — see [21], [22] for more details. Using the latter nonsmooth calculus tool, Theorem 1 is generalized as follows.

Theorem 2: Consider the differential equation in (1) with f locally Lipschitz. The following hold:

- A set $H \subset \mathbb{R}^n$ is conditionally invariant with respect to $F \subset H$ if there exists a locally Lipschitz function $\delta : \mathbb{R}^n \to \mathbb{R}$ such that

$$\begin{aligned} \langle \partial_P \delta(x), f(x) \rangle &\leq 0 \quad \forall x \in U(H), & (23)\\ \delta(x) - \delta(y) &< 0 \quad \forall (x,y) \in \partial F \times (U(H)\backslash H). & (24) \end{aligned}$$

- A set H is strictly conditionally invariant with respect to $F \subset \text{int}(H)$ if there exists a locally Lipschitz function $\delta : \mathbb{R}^n \to \mathbb{R}$ such that

$$\begin{aligned} \langle \partial_P \delta(x), f(x) \rangle &\leq 0 \qquad \forall x \in H, & (25)\\ \delta(x) - \delta(y) &< 0 \qquad \forall (x,y) \in \partial F \times \partial H. & (26) \end{aligned}$$

□

IV. Necessary and sufficient conditions for safety

In this section, we construct a barrier function for safe systems using the converse theory for non-asymptotic Lyapunov stability. Converse theory for (non-asymptotic) Lyapunov stability has been developed during the 40-50's by the eastern control community, see [15], [16], [17], [18], [19], and [23] for an overview on this topic. Based on this background, we first show, using a counter-example, that in some cases we cannot construct an autonomous and continuous barrier function certifying safety according to any of the existing characterizations, even if the system is safe, smooth, and autonomous. The considered counter-example can be found in [19, Example 21.14, page 82] and [18, Remark, Page 46], where the objective was to show that some stable systems do not admit a continuous and autonomous Lyapunov function that is nonincreasing along the system's solutions.

Example 2: Consider the two dimensional system

$$\begin{aligned} \dot{x}_1 &= -x_2 + r x_1 \sin(1/r) \\ \dot{x}_2 &= x_1 + r x_2 \sin(1/r), \quad r = |x|. \end{aligned} \quad (27)$$

In polar coordinates, this system can be rewritten as

$$\dot{r} = r^2 \sin(1/r), \qquad \dot{\theta} = 1. \quad (28)$$

The system in the original coordinates is safe with respect to the sets

$$X_o := \{0\}, \quad X_u := \mathbb{R}^2 \backslash X_o.$$

[1]By $\delta \in \mathcal{C}^o \cap \mathcal{C}^1(U(H)\backslash F)$, we mean that δ is continuous on its domain of definition, and continuously differentiable on the set $U(H)\backslash F$.

Indeed, the safety property in this case is equivalent to forward invariance of the origin (which coincides with X_o). Forward invariance of the origin holds since the origin is an equilibrium point for system (27). However, we will show that it is not possible to find a continuous barrier candidate B, function only of x, that is nonincreasing along the system's solutions and at the same time having a value at the origin that is strictly smaller than all the values elsewhere. Indeed, from (28), in the phase portrait of (27), the origin is surrounded by (countably) infinitely many limit cycles centered at the origin, denoted by Q_k, $k \in \mathbb{N}$. Moreover, the radius of the limit cycles converges to zero as $k \to \infty$ and the trajectories starting from the interior of the torus formed by each two circles Q_{k+1} and Q_k are spirals that leave Q_{k+1} and approach Q_k. This being said, we assume the existence of a continuous function B that is nonincreasing along the system's solutions and positive definite. Furthermore, for a sequence of points $\{x_k\}_{k=0}^{\infty}$ with $x_k \in Q_k$, the sequence $\{B(x_k)\}_{k=0}^{\infty}$ converges to zero, and is strictly positive. Hence, there exists a strictly positive and monotonically decreasing subsequence $\{B(x_{k_i})\}_{i=0}^{\infty}$ that also converges to zero. As a result, there exist $(l_1, l_2) \in \mathbb{N}\times\mathbb{N}$ and $\epsilon > 0$ such that $B(x_{l_1}) - B(x_{l_2}) = \epsilon$. We assume, further and without loss of generality, that $l_2 - l_1 = 2$ (the same reasoning is valid if $l_2 - l_1 > 2$). Next, using the continuity assumption on B and the system's behavior, it follows that for any $\epsilon_1 > 0$ we can find $T > 0$ and two initial conditions x_o and x_{o1} in the interior of the torus formed by Q_{l_2} and Q_{l_2-1} and, respectively, in the interior of the torus formed by Q_{l_2-1} and Q_{l_1} such that

$$\max\{|B(x_o) - B(x_{l_2})|,\ |B(x_{o1}) - B(x(T, x_o))|, \\ |B(x_{l_1}) - B(x(T, x_{o1}))|\} \leq \epsilon_1.$$

Now, having

$$\begin{aligned}\epsilon = &B(x_{l_1}) - B(x_{l_2}) = B(x_{l_1}) - B(x(T, x_{o1})) + \\ &B(x(T, x_{o1})) - B(x_{o1}) + B(x_{o1}) - B(x(T, x_o)) + \\ &B(x(T, x_o)) - B(x_o) + B(x_o) - B(x_{l_2})\end{aligned}$$

and using the fact that B does not increase along the system's solutions, we obtain

$$\begin{aligned}\epsilon = &B(x_{l_1}) - B(x_{l_2}) \leq |B(x_{l_1}) - B(x(T, x_{o1}))| + \\ &|B(x_{o1}) - B(x(T, x_o))| + |B(x_o) - B(x_{l_2})| \leq 3\epsilon_1.\end{aligned}$$

The latter fact yields a contradiction since ϵ is fixed and ϵ_1 can be made as small as possible, that is, for $\epsilon_1 = \epsilon/4$, we obtain $\epsilon \leq 3\epsilon/4$ which is a contradiction. Hence, though it is safe, an autonomous barrier certificate does not exist for this system. □

Before presenting our main results on the existence of time-varying barrier certificates for safe systems, the following remarks are in order.

Remark 3: In [15], Persidskii proposed, for the first time, a construction of a continuous time-varying Lyapunov function that does not increase along the system's solutions and that is positive definite provided that the origin is (uniformly) stable, the system's solutions are locally bounded, and the vector field is continuous. Later on, Krasovskii and Kurzweil refined this construction in [16] and [18], respectively. Consequently, they deduced the existence of a continuously differentiable time-varying and nonincreasing (along the system's solutions) Lyapunov function that is positive definite provided that the origin is stable (uniformly), the vector field is continuously differentiable, and the system's solutions are locally bounded. A remarkable extension of those results is in [17], where the authors showed the existence of a smooth (of any order of smoothness) time-varying positive definite Lyapunov function which is nonincreasing (along the system's solutions) provided that the vector field is only continuous, the solutions locally bounded, and the origin (uniformly) stable. However, the latter reference is available only in Russian, and we are still wondering whether it can help improving the constructions of barrier certificates we are presenting in this paper. •

Remark 4: It is worth stressing that the concept of Lyapunov stability is equivalent to conditional invariance of a converging sequences of compact sets [17]. However, extending the aforementioned results to the context of conditional invariance (or, safety) is not straightforward and offers many technical challenges. Those challenges are related to the fact that the sets F and H are not necessarily compact, they are not necessarily forward invariant, and the system's solutions are not necessarily bounded nor complete. Consequently, for a general safe system, most of the existing constructions from the context of Lyapunov stability cannot be extended to the context of safety. •

In the following statement, we show that when the system's dynamics is locally Lipschitz and when the solutions are forward complete, conditional invariance (equivalently, safety) is equivalent to the existence of a locally Lipschitz time-varying barrier-like function certifying this property.

Theorem 3: Consider the system (1) with f locally Lipschitz. Assume further that every maximal solution to (1) is complete. The following hold:

- A set $H \subset \mathbb{R}^n$ is conditionally invariant with respect to $F \subset H$ if and only if there exists a locally Lipschitz function $\delta : \mathbb{R}_{\geq 0} \times \mathbb{R}^n \to \mathbb{R}$ such that

$$\langle \partial_P \delta(t, x), [1 \quad f(x)^\top]^\top \rangle \leq 0 \qquad \forall x \in \mathbb{R}^n, \tag{29}$$

$$\delta(0, x) - \delta(t, y) < 0 \\ \forall (t, x, y) \in \mathbb{R}_{\geq 0} \times \partial F \times (U(H)\backslash H). \tag{30}$$

- A set $H \subset \mathbb{R}^n$ is strictly conditionally invariant with respect to $F \subset \text{int}(H)$ if and only if there exists a locally Lipschitz function $\delta : \mathbb{R}_{\geq 0} \times \mathbb{R}^n \to \mathbb{R}$ such that (29) holds and

$$\delta(0, x) - \delta(t, y) < 0 \ \ \forall (t, x, y) \in \mathbb{R}_{\geq 0} \times \partial F \times \partial H. \tag{31}$$

□

Remark 5: The completeness requirement of the systems solutions plays an important role to show the Lipschitz continuity of the constructed barrier candidate when the system is conditionally invariant. Relaxing the completeness requirement is part of our future research. •

In the case of stability of the origin, Kurzweil in [16] deduced from the Lyapunov function constructed in [15] the existence of a Lyapunov function that is $\mathcal{C}^1$ everywhere (except at the origin) under the $\mathcal{C}^1$ regularity of the vector field and the fact that the origin is an equilibrium point. The compactness of the origin is an important requirement for its proof to hold. Unfortunately, this assumption does not hold when a generic (not invariant) set is considered instead of the origin. However, we can handle such situation by extending [19, Lemma 48.3]. It should be added that the origin being an equilibrium plays an important role in [16] to guarantee positive definiteness of a certain function used in the proof. However, in our case, when the origin is replaced by a generic closed set, such a function is not necessarily positive definite. Therefore, to handle this situation, we propose a state dependent change in the system's time scale such that, in the new time scale, this function becomes positive definite.

Theorem 4: Consider system (1) with $f \in \mathcal{C}^1$. Assume further that every maximal solution to it is complete. Then, system (1) is safe with respect to given sets (X_o, X_u) if and only if there exists a function $B : \mathbb{R}_{\geq 0} \times \mathbb{R}^n \to \mathbb{R}$ of class $\mathcal{C}^o \cap \mathcal{C}^1\left((\mathbb{R}_{\geq 0} \times \mathbb{R}^n)\backslash K\right)$, where $K := \{(t,x) \in \mathbb{R}_{\geq 0} \times \mathbb{R}^n : B(t,x) \leq 0\}$, such that

$$\begin{cases} B(t,x) > 0 & \forall x \in X_u \quad \forall t \in \mathbb{R}_{\geq 0}, \\ B(t,x) \leq 0 & \forall x \in X_o \quad \forall t \in \mathbb{R}_{\geq 0}, \\ \frac{\partial B}{\partial t}(t,x) + \frac{\partial B}{\partial x}(t,x) f(x) \leq 0 & \forall (t,x) \in (\mathbb{R}_{\geq 0} \times \mathbb{R}^n) \backslash K. \end{cases} \tag{32}$$

□

Remark 6: The forward completeness requirement in the previous statement is important for the barrier function therein to exist, when the system is safe, and to be well defined. Relaxing the completeness in the proposed framework is an open question and may involve a completely different construction of the barrier function than the one we propose. •

V. CONCLUSION

In this paper, we proposed sufficient and necessary conditions for safety (equivalently, conditional invariance) using barrier-like functions. The first part of the paper relaxed existing sufficient conditions. The proposed relaxations concern the sign and the regularity of the considered barrier-like functions. In the second part, guided by the lack of existence of autonomous and continuous barrier functions certifying safety in a class of safe systems, time-varying barrier-like functions certifying safety are proposed and there existence is shown to be both necessary as well as sufficient. The regularity of the proposed time-varying barrier-like functions depends on the regularity of the system's dynamics. Our approach is inspired by converse Lyapunov theorems for only stability.

REFERENCES

[1] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Transactions on Automatic Control*, vol. 52, no. 8, pp. 1415–1428, 2007.

[2] G. S. Ladde and V. Lakshmikantham, "On flow-invariant sets.," *Pacific Journal of Mathematics*, vol. 51, no. 1, pp. 215–220, 1974.

[3] G. S. Ladde and S. Leela, "Analysis of invariant sets," *Annali di Matematica Pura ed Applicata*, vol. 94, no. 1, pp. 283–289, 1972.

[4] V. Lakshmikantham and S. Leela, *Differential and Integral Inequalities: Theory and Applications*, vol. I. Academic press, New York, 1969.

[5] A. A. Kayande and V. Lakshmikantham, "Conditionally invariant sets and vector lyapunov functions," *Journal of Mathematical Analysis and Applications*, vol. 14, no. 2, pp. 285–293, 1966.

[6] D. Belleter, M. Maghenem, C. Paliotta, and K. Y. Pettersen, "Observer based path following for underactuated marine vessels in the presence of ocean currents: A global approach," *Automatica*, vol. 100, pp. 123 – 134, 2019.

[7] H. G. Tanner, A. Jadbabaie, and G. J. Pappas, "Stable flocking of mobile agents, Part I: Fixed topology," in *42nd Conference on Decision and Control*, vol. 2, pp. 2010–2015, IEEE, 2003.

[8] A. G. Wills and W. P. Heath, "Barrier function based model predictive control," *Automatica*, vol. 40, no. 8, pp. 1415 – 1422, 2004.

[9] K. P. Tee, S. S. Ge, and E. H. Tay, "Barrier lyapunov functions for the control of output-constrained nonlinear systems," *Automatica*, vol. 45, no. 4, pp. 918–927, 2009.

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

[12] S. Prajna and A. Rantzer, "On the necessity of barrier certificates," *IFAC Proceedings Volumes*, vol. 38, no. 1, pp. 526–531, 2005.

[13] R. Wisniewski and C. Sloth, "Converse barrier certificate theorems," *IEEE Transactions on Automatic Control*, vol. 61, no. 5, pp. 1356–1361, 2016.

[14] X. Xu, "Constrained control of input−output linearizable systems using control sharing barrier functions," *Automatica*, vol. 87, pp. 195 – 201, 2018.

[15] K. P. Persidskii, "On a theorem of Liapunov," *C. R. (Dokl.) Acad. Sci. URSS*, vol. 14, pp. 541–543, 1937.

[16] J. Kurzweil, "On the inversion of Lyapunov's first theorem on the stability of motion (In Russian)," *Czechoslovak Mathematical Journal*, vol. 5, no. 3, pp. 382–398, 1955.

[17] J. Kurzweil and I. Vrkoč, "Transformation of Lyapunov's theorems on stability and Persidskii's theorems on uniform stability (In Russian)," *Czechoslovak Mathematical Journal*, vol. 7, no. 2, pp. 254–272, 1957.

[18] N. N. Krasovskii, *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, 1963.

[19] W. Hahn, *Stability of Motion*, vol. 138. Springer, 1967.

[20] S. Prajna, *Optimization-based methods for nonlinear and hybrid systems verification*. PhD thesis, California Institute of Technology, 2005.

[21] F. H. Clarke, *Optimization and Nonsmooth Analysis*, vol. 5. 1990.

[22] F. H. Clarke, Y. S. Ledyaev, R. J. Stern, and P. R. Wolenski, *Nonsmooth Analysis and Control Theory*, vol. 178. Springer Science & Business Media, 2008.

[23] C. M. Kellett, "Classical converse theorems in Lyapunov's second method.," *Discrete & Continuous Dynamical Systems-Series B*, vol. 20, no. 8, 2015.