SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

March 2023, Vol. 66 132102:1–132102:15
https://doi.org/10.1007/s11432-020-3266-6

Safety guarantee for time-delay systems with disturbances

Wenyou LIU[1,2], Yunjun BAI[1,2], Li JIAO[1,2*] & Naijun ZHAN[1,2*]

[1]*State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing* 100190*, China;*
[2]*University of Chinese Academy of Sciences, Beijing* 100049*, China*

Received 18 November 2020/Revised 25 February 2021/Accepted 13 May 2021/Published online 18 January 2023

Abstract Time delays occur in various engineering applications because they may be inherent in the plants or caused by networks. In this paper, we investigate the safety verification problem of time-delay systems modeled by nonlinear delay differential equations subject to control inputs and disturbances in their dynamics. Building upon classical control barrier functionals, we develop the notions of input-to-state safety and input-to-state safe control barrier functionals, in which input-to-state safe control barrier functionals are used to guarantee the safety of time-delay systems with control inputs and disturbances. Three examples are provided to demonstrate the proposed approach.

Keywords time-delay systems, delay differential equations, control barrier functionals, controllers, safety

Citation Liu W Y, Bai Y J, Jiao L, et al. Safety guarantee for time-delay systems with disturbances. Sci China Inf Sci, 2023, 66(3): 132102, https://doi.org/10.1007/s11432-020-3266-6

1 Introduction

Cyber-physical systems (CPSs), such as smart grids [1], intelligent traffic systems [2], and smart factories [3], have emerged and are applied in our daily lives. Many of these systems are safety-critical, i.e., any fault in them may result in severe property damage, injuries, and even loss of life. Consequently, it is essential to ensure the safety of these systems before deploying them.

Time delays are intrinsic in many real systems. For instance, due to the limitation of reproductive age and food regeneration, the growth rate of biological species depends on the number of present and past species [4]. The latent period of some infectious diseases introduces a delay in their transmission process [5]. Over the past decades, increasing attention has been paid to time-delay systems because of their broad applications in engineering, such as chemical process control [6], human balancing [7], communications [8], and neural network systems [9]. Delay differential equations (DDEs), as a new model with an explicit dependence of the dynamics on past states in the differential equation framework, have been developed, e.g., by Myschkis [10] and Bellman and Cooke [11], to study the dynamics of time-delay systems.

Over the past decades, methodologies for studying stability analysis of time-delay systems have been extensively studied such as H_∞- and L_2-stability theories [12], absolute stability [13] and input-to-state stability. In contrast, methodologies for safety analysis ensuring the safety of time-delay systems are few. One is the barrier certificate (BC) based method. A BC can separate all reachable states of a considered system from a given unsafe set, thus ensuring that the system is safe. It was originally developed for the safety verification of systems free of time delays modeled by ordinary differential equations (ODEs) in [14], and afterward extended to systems with control inputs in [15, 16] and time-delay (hybrid) systems [17, 18]. However, time-delay systems considered in [17, 18] are free of disturbances in their dynamics. Due to unknown and changing external and/or internal factors, disturbances are ubiquitous in many engineering systems such as wind forces [19], pedestrian systems [20], option systems [21], and biological systems [22].

[*] Corresponding author (email: ljiao@ios.ac.cn, znj@ios.ac.cn)

The presence of disturbances further complicates the safety verification of time-delay systems. Existing BC-based approaches cannot be applied to systems subject to both time delays and disturbances.

In this paper, the safety verification problem of time-delay systems modeled by DDEs subject to control inputs and disturbances is investigated. We first propose input-to-state safe control barrier functionals (ISSf-CBFs), whose existence can guarantee the safety of time-delay systems subject to control inputs and disturbances, and then present an algorithm for synthesizing ISSf-CBFs. Finally, we demonstrate our method with three examples.

The main contributions are summarized as follows.

- We lift the BC-method for ODEs to safety verification of DDEs subject to control inputs and disturbances.
- ISSf-CBFs are developed to guarantee the safety of time-delay systems with control inputs and disturbances.
- We demonstrate the theoretical developments of the proposed method with three examples.

The remainder of this paper is organized as follows. Section 2 gives an introduction to related studies. Section 3 introduces basic notions used throughout this paper, including time-delay systems and the safety problem of interest. Section 4 develops the notion of CBFs to verify the safety of time-delay systems with control inputs but without disturbances. Section 5 presents the safety guarantee for time-delay systems with control inputs and disturbances. Three examples are given in Section 6 to demonstrate the theoretical developments of our method. Finally, we conclude this paper and discuss future studies in Section 7.

2 Related work

As surveyed in [23], various approaches have been proposed to verify the safety properties of CPSs during the past decades, driven by the demand for safety-critical CPS design. Among these, BC-based approaches [14] are very promising and are closely related to this work. A BC can divide the state space of a considered system into safe and unsafe parts, according to the safety properties to be verified, and ensure that all reachable states are safe. Automatic generation of BCs is the cornerstone of BC-based approaches, which can be reduced to constraint solving problems and further solved by convex optimization-based approaches when the considered system is polynomial. Since [14], increasing attention has been paid to the synthesis of more expressive BCs via constructing less conservative convex conditions, e.g., exponential conditions [24], Darboux conditions [25], general relaxed-barrier certificate conditions [26], and vector-barrier certificate conditions [27]. However, it is still open whether the necessary and sufficient condition of a formula being an inductive invariant given in [28] can be used as the weakest BC condition, according to which synthesizing BCs can be done with convex optimization.

To handle safety verification of dynamic systems with control inputs, Refs. [15, 16] extended BCs to control barrier certificates (CBCs) and presented convex optimization-based approaches to synthesizing CBCs. Also, BC-based approaches were extended to time-delay systems [17, 18, 29], which are free of control inputs and disturbances.

Recently, automatic verification of CPSs with time delays has drawn growing attention. A few other approaches have also been proposed. Refs. [30, 31] investigated how to construct symbolic abstraction of time-delay systems with control inputs by exploiting input-to-state stability so that the verification of time-delay systems can be reduced to the reachability problem of finite state machines. In [32], the authors considered the verification of networked-dynamical systems with time delays associated with discrete jumps between different modes by computing reachable sets of ODEs with uncertain inputs. This computation is achieved by simulation together with sensitivity analysis over bounded time horizons. Refs. [33,34] attempted exploiting local-homeomorphism properties of DDEs to compute inner- and outer-approximations of their reachable sets in bounded time horizons, similar to the set boundary analysis method for ODEs in [35]. Recently, a Taylor model-based approach was proposed to over- and under-approximate reachable sets of DDEs with uncertain parameters and initial states in [36]. To conduct unbounded verification of DDEs, Refs. [37] proposed an approach based on interval Taylor models and stability analysis for a class of simple DDEs, and Refs. [38] proposed a Lyapunov function-based approach. Recently, a method was proposed for analyzing the safety of exponentially stable time-delay systems using linearization and spectral analysis [29].

All the aforementioned approaches cannot handle safety verification of time-delay systems with control inputs and disturbances over the unbounded time horizon. In contrast, ISSf-CBFs proposed in this paper can be used to guarantee the safety of time-delay systems subject to control inputs and disturbances.

3 Preliminaries

Let $\mathbb{R}$ denotes the set of real numbers, and $\mathbb{R}_{\geqslant 0}$ denotes the set of non-negative real numbers. Given a vector $x \in \mathbb{R}^n$, $|x|$ denotes its Euclidean norm. For $d(\cdot) : \mathbb{R}_{\geqslant 0} \to \mathbb{R}^m$, its $\mathbb{L}_\infty^m$ norm is given by $\|d\|_\infty := \operatorname{ess\,sup}_t |d(t)|$, where ess sup denotes the essential supremum (see Definition 1). Given a set $\mathcal{I} \subseteq \mathbb{R}^n$, let $\partial\mathcal{I}$, $\mathrm{Int}(\mathcal{I})$, and $\overline{\mathcal{I}}$ denote the boundary, interior, and closure of $\mathcal{I}$, respectively. For given constants $a, b \in \mathbb{R}$ with $a \leqslant b$, let $\mathcal{B}([a,b], \mathbb{R}^n)$ denote the space of functions mapping from the interval $[a,b]$ to $\mathbb{R}^n$.

Definition 1 (Essential supremum)**.** Given a measurable function $d(\cdot) : T \to \mathbb{R}$, where T is a measure space with measure μ. The essential supremum "ess sup" of d is the smallest number c such that the set $\{t \in T \mid d(t) > c\}$ has measure zero.

Definition 2 (Dirac delta function [39])**.** Dirac delta function is a linear functional from a space of test function f. The action of δ on f, commonly denoted $\delta[f]$ or $\langle \delta, f\rangle$, then gives the value at 0 of f for any function f, and has the following property:

$$\int_{-\infty}^{+\infty} f(x)\delta(x-a)\mathrm{d}x = f(a).$$

Definition 3 (Class $\mathcal{K}$ function)**.** Given a constant $a > 0$ and a function $\alpha : [0, a) \to [0, +\infty)$, if α is continuous, strictly increasing with $\alpha(0) = 0$, then we say α is a class $\mathcal{K}$ function, i.e., $\alpha \in \mathcal{K}$.

The following notions will be used throughout this paper.

- Given a function $\alpha : (-b, c) \to (-\infty, +\infty)$, if α is continuous, strictly increasing with $\alpha(0) = 0$ for some $b > 0$ and $c > 0$, then we say α is an extended class $\mathcal{K}$ function. Here b, c can be $+\infty$.
- Given a function $\alpha : [0, +\infty) \to [0, +\infty)$, if α is continuous, strictly increasing with $\alpha(0) = 0$, and $\alpha(r) \to +\infty$ as $r \to +\infty$, then we say α is a class $\mathcal{K}_\infty$ function.
- Given a continuous function $\gamma : \mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$, if given a fixed n, $\gamma(m,n)$ belongs to class $\mathcal{K}$ with respect to m, and given a fixed m, $\gamma(m,n)$ is decreasing with respect to n and $\lim_{n\to\infty} \gamma(m,n) = 0$, then we say γ is a class $\mathcal{KL}$ function.

In this paper we consider time-delay systems described by DDEs of the following form:

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

where $x \in \mathbb{R}^n$ is the system state, $d(\cdot) : \mathbb{R}_{\geqslant 0} \to \mathbb{R}^m$ is the input disturbance, $u(\cdot) : \mathbb{R}_{\geqslant 0} \to U \subset \mathbb{R}^m$ is the control input, $f : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ is continuous and satisfies the local Lipschitz condition, $g : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^{n\times m}$ is continuous and satisfies the local Lipschitz condition, and τ is the time delay term. We define a function $x_t(\omega) = x(t+\omega)$, $\omega \in [-\tau, 0]$, in the Banach space $\mathcal{B}^\tau = \mathcal{B}([-\tau, 0], \mathbb{R}^n)$, which maps the time interval $[-\tau, 0]$ to $\mathbb{R}^n$. The initial condition of system (1) is a function $x_0(\omega) = x(\omega)$, $\omega \in [-\tau, 0]$, rather than a single state $x(0)$ as in ODEs.

Note that system (1) is similar to the ones considered in [16], both of them considered the issues of control inputs and disturbances, but Ref. [16] did not consider the existence of time delays.

System (1) can be transformed into the following functional differential equation:

$$\dot{x}(t) = \mathcal{F}(x_t) + \mathcal{G}(x_t)(u(t) + d(t)), \tag{2}$$

where the functionals $\mathcal{F} : \mathcal{B}^\tau \to \mathbb{R}^n$ and $\mathcal{G} : \mathcal{B}^\tau \to \mathbb{R}^{n\times m}$ are defined as follows:

$$\mathcal{F}(\psi) = f(\mathcal{R}_0(\psi), \mathcal{R}_{-\tau}(\psi)), \quad \mathcal{G}(\psi) = g(\mathcal{R}_0(\psi), \mathcal{R}_{-\tau}(\psi)), \tag{3}$$

where

$$\mathcal{R}_\sigma(\psi) = \int_{-\tau}^{0} \psi(\omega)\delta(\omega - \sigma)\mathrm{d}\omega = \psi(\sigma),$$

and δ stands for the Dirac delta function.

Given an initial condition $x_0 = x_0(\omega) \in \mathcal{B}^\tau, \omega \in [-\tau, 0]$, due to the assumption of local Lipschitz condition, system (1) or (2) has a unique solution $x_t(\omega) : [0, t_{\max}) \to \mathbb{R}^n$, where $\omega \in [-\tau, 0]$ and $t_{\max}$ is the maximal execution time of (1). In the case that (2) is forward complete, then $t_{\max} = +\infty$. If for all $x_0(0) \in \mathcal{S}$, $x_t(0) \in \mathcal{S}$ for $t < t_{\max}$, then we call that $\mathcal{S} \subset \mathbb{R}^n$ is forward invariant. In this study, a set $\mathcal{S}$ is called a safe set if $\mathcal{S}$ is forward invariant.

4 Control barrier functionals

The notions of BCs and CBCs are extensively applied in the verification of dynamical and hybrid systems whose continuous dynamics are described by ODEs [14, 15]. In recent years, a similar idea to BC based approaches was adapted to verifying the safety of DDEs, i.e., barrier functional (BF) based approach [17, 18]. In [30, 31], the notion of CBC was also extended to DDEs, called control barrier functionals (CBFs), for stability analysis. In this section, we generalize CBFs for DDEs stability analysis to the verification of DDEs, and generate safe controllers based on CBFs.

4.1 Barrier functionals

In this subsection, we mainly recall the notion of BFs. BFs, which are used to ensure the safety of nature time-delay systems, were first proposed in [14] and were further investigated later in [18]. The idea of barrier functionals is similar to Lyapunov-Krasovskii functionals used in the stability analysis of DDEs.

Considering the time-delay system (1) without the term $g(x(t), x(t-\tau))(u(t)+d(t))$[1], i.e.,

$$\dot{x}(t) = f(x(t), x(t-\tau)).$$

As discussed in Section 3, it can be transformed into a functional differential equation of the following form:

$$\dot{x}(t) = \mathcal{F}(x_t). \tag{4}$$

For ease of exposition, let's fix a set $\mathcal{C}$ and its boundary and interior, given by

$$\mathcal{C} = \{\psi \in \mathcal{B}^\tau : \mathcal{H}(\psi) \geqslant 0\}, \tag{5}$$

$$\partial\mathcal{C} = \{\psi \in \mathcal{B}^\tau : \mathcal{H}(\psi) = 0\}, \tag{6}$$

$$\mathrm{Int}(\mathcal{C}) = \{\psi \in \mathcal{B}^\tau : \mathcal{H}(\psi) > 0\}, \tag{7}$$

where $\mathcal{H} : \mathcal{B}^\tau \to \mathbb{R}$ is a continuously differentiable functional. Clearly, $\overline{\mathcal{C}} = \mathcal{C}$. We assume that $\mathrm{Int}(\mathcal{C})$ is non-empty in what follows.

If the set $\mathcal{C}$ is forward invariant, then the system (4) is safe with respect to $\mathcal{C}$. Lemma 1 in [18] presents conditions making $\mathcal{C}$ be forward invariant.

Lemma 1 ([18])**.** For a time-delay system (4) and a set $\mathcal{C} \subset \mathcal{B}^\tau$ defined as (5)–(7), if there exists $\alpha \in \mathcal{K}_{(-b,c)}$ for some $b, c \in \mathbb{R}_{\geqslant 0}$ satisfying

$$\dot{\mathcal{H}}(x_t) \geqslant -\alpha(\mathcal{H}(x_t)), \tag{8}$$

where $\dot{\mathcal{H}}(x_t)$ is the derivative of functional $\mathcal{H}$ with respect to t, i.e., $\dot{\mathcal{H}}(x_t) = \mathrm{d}\mathcal{H}(x_t)/\mathrm{d}t$, then we say the set $\mathcal{C}$ is forward invariant.

Lemma 1 gives a condition, which implies that any trajectory originating from $\mathcal{C}$ cannot punch through its boundary, to ensure the safety of the time-delay system (4) with respect to the set $\mathcal{C}$. A functional $\mathcal{H}$ satisfying condition (8) is called barrier functional, which can guarantee the safety of time-delay system (4) with respect to the set $\mathcal{C}$.

Additionally, as $\alpha \in \mathcal{K}_{(-b,c)}$, the choice of b and c should guarantee $\mathcal{H}(x_t) \in (-b, c)$. So, in practice, they can be defined as

$$b := -\inf_{x_t \in \mathcal{B}^\tau} \mathcal{H}(x_t), \quad c := \sup_{x_t \in \mathcal{B}^\tau} \mathcal{H}(x_t). \tag{9}$$

[1] Note that we use a DDE with a single constant time delay as an instance for illustration. However, it can be easily generalized to DDEs with multiple delays.

4.2 Control barrier functionals

By taking control inputs into account, the controlled time-delay system of interest is given below:

$$\dot{x}(t) = f(x(t), x(t-\tau)) + g(x(t), x(t-\tau))u(t),$$

where $f : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ and $g : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^{n\times m}$ are locally Lipschitz, $x \in \mathbb{R}^n$ denotes the system state, $u : \mathbb{R}_{\geqslant 0} \to U \subset \mathbb{R}^m$ denotes the control input, and the constant $\tau \in \mathbb{R}_{\geqslant 0}$ denotes the time delay. Similarly, the system can be rewritten as a functional differential equation of the following form:

$$\dot{x}(t) = \mathcal{F}(x_t) + \mathcal{G}(x_t)u(t), \tag{10}$$

where $\mathcal{F} : \mathcal{B}^\tau \to \mathbb{R}^n$ and $\mathcal{G} : \mathcal{B}^\tau \to \mathbb{R}^{n\times m}$ are functionals defined in (3).

In order to verify a time-delay system with control inputs of the form (10), we extend the notion of barrier functionals to the one of control barrier functionals.

Definition 4 (CBFs)**.** Consider a time-delay system of (10), let $\mathcal{C} \subset \mathcal{B}^\tau$ be a set defined as (5)–(7), if there exists an $\alpha \in \mathcal{K}_{(-b,c)}$ for some $b, c \in \mathbb{R}_{\geqslant 0}$ such that $\forall x_t \in \mathcal{C}$,

$$\sup_{u(t)\in U} [\dot{\mathcal{H}}(x_t)] \geqslant -\alpha(\mathcal{H}(x_t)), \tag{11}$$

then $\mathcal{H}$ is called control barrier functional.

Note that the above definition is similar to the notion of δ-ISS Lyapunov-Krasovskii functional defined in [30, 31], which is used for stability analysis of DDEs. We will prove in the following theorem (i.e., Theorem 1) that the control values satisfying constraint (11) can guarantee the safety of time-delay systems with relative degree one (i.e., $\mathcal{H}_\mathcal{G}(x_t) \neq 0$). Before presenting Theorem 1 we need the following auxiliary lemma.

Lemma 2 (Comparison theory [40])**.** For a scalar differential equation as follows:

$$\dot{y} = f(t, y), \quad y(t_0) = y_0,$$

where for all $t \geqslant 0$ and all $y \in J \subset \mathbb{R}$, $f(t, y)$ is locally Lipschitz in y and continuous in t. Let $[t_0, t_{\max})$ ($t_{\max}$ could be ∞) be the time interval over which the solution $y(t)$ exists; moreover assume $y(t) \in J$. Let $n(t)$ be a continuous function and for all $t \in [t_0, t_{\max})$, the following inequality holds:

$$D^+n(t) \geqslant f(t, n(t)),\ n(t_0) \geqslant y_0$$

with $n(t) \in J$, where $D^+n(\cdot)$ is the upper right-hand derivative of $n(t)$. Then, $n(t) \geqslant y(t)$ holds for all $t \in [t_0, t_{\max})$.

Theorem 1. For the time-delay system (10), a set $\mathcal{C} \subset \mathcal{B}^\tau$ is defined as (5)–(7), if $\mathcal{H}$ is a control barrier functional, then $\mathcal{C}$ is forward invariant.

Proof. Let

$$\dot{z}(t) = -\alpha(z(t)),\ z(0) = \mathcal{H}(x_0). \tag{12}$$

According to the existence and uniqueness theorem for ODEs, there is a unique solution to (12), say

$$z(t) = \gamma(z(0), t) = \gamma(\mathcal{H}(x_0), t)$$

for all $t \geqslant 0$. Since α is a class $\mathcal{K}$ function, we can get that γ is decreasing with respect to t for a fixed $\mathcal{H}(x_0)$ and γ is a class $\mathcal{K}$ function for a fixed t. Therefore, γ satisfies the properties of class $\mathcal{KL}$ function [41]. Applying Lemma 2 for (11) and (12), we get

$$\mathcal{H}(x_t) \geqslant \gamma(\mathcal{H}(x_0), t)$$

for $0 \leqslant t < t_{\max}$. According to the property of class $\mathcal{KL}$ function, we have for $0 \leqslant t < t_{\max}$, $\mathcal{H}(x_t) \geqslant 0$. Hence, $\mathcal{C}$ is forward invariant.

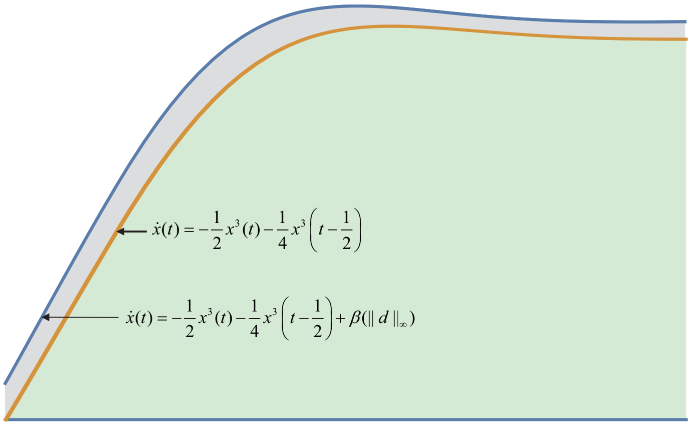
$\dot{x}(t)=-\frac{1}{2}x^3(t)-\frac{1}{4}x^3\left(t-\frac{1}{2}\right)$
$\dot{x}(t)=-\frac{1}{2}x^3(t)-\frac{1}{4}x^3\left(t-\frac{1}{2}\right)+\beta(\|d\|_\infty)$

Figure 1 (Color online) An example of the safe set $\mathcal{C}$ and the corresponding input-to-state safe set $\mathcal{C}_d$. The green region is the set $\mathcal{C}$, green + grey region is set $\mathcal{C}_d$.

5 Safety guarantee under disturbances

In this section, we study the input-to-state safety for DDEs with disturbances. Suppose that we already have a safekeeping controller $k(x(t))$ for system (10), which could be contaminated by some disturbances $d(t)$, i.e., $k(x(t))+d(t)$. As a result, we need to consider a system of the following form:

$$\dot{x}(t)=\mathcal{F}(x_t)+\mathcal{G}(x_t)(k(x(t))+d(t)), \tag{13}$$

where $x_t(\omega)=x(t+\omega)$ for $\omega\in[-\tau,0]$ and $d(\cdot):\mathbb{R}_{\geqslant 0}\rightarrow\mathbb{R}^m$.

5.1 Input-to-state safety

The concept of input-to-state safety is utilized for analyzing the safety properties of systems. It was first proposed in [42], and then in [43]. They aim to keep the underlying system away from the unsafe state set $\mathcal{S}_u\subset\mathbb{R}^n$. While Ref. [16] redefined the concept of input-to-state safety, requiring the system to evolve in the safe set $\mathcal{S}$. We try to construct a controller to ensure that the system is input-to-state safe, which is similar to the approach of constructing input-to-state stabilizing controllers in [44]. To guarantee the safety property, the goal is to ensure that the system always evolves in the set $\mathcal{C}$, or at least close to the set $\mathcal{C}$. The closeness to set $\mathcal{C}$ is related to the size of disturbances.

If a set $\mathcal{C}$ is forward invariant, the set $\mathcal{C}$ is called safe. Similarly, if there exists a set $\mathcal{C}_d\supseteq\mathcal{C}$ such that the set $\mathcal{C}_d$ is forward invariant, the set $\mathcal{C}$ is input-to-state safe. The set $\mathcal{C}_d$ is defined as

$$\mathcal{C}_d=\{\psi\in\mathcal{B}^\tau:\mathcal{H}(\psi)+\beta(\|d\|_\infty)\geqslant 0\}, \tag{14}$$
$$\partial\mathcal{C}_d=\{\psi\in\mathcal{B}^\tau:\mathcal{H}(\psi)+\beta(\|d\|_\infty)=0\}, \tag{15}$$
$$\mathrm{Int}(\mathcal{C}_d)=\{\psi\in\mathcal{B}^\tau:\mathcal{H}(\psi)+\beta(\|d\|_\infty)>0\}, \tag{16}$$

where $\beta\in\mathcal{K}_{[0,a)}$ with a satisfying $\lim_{r\rightarrow a}\beta(r)=b$ and $\|d\|_\infty\leqslant\bar{d}\in[0,a)$. Clearly, $\overline{\mathcal{C}_d}=\mathcal{C}_d$. We also assume $\mathrm{Int}(\mathcal{C}_\mathrm{d})$ is non-empty. The relationship between the safe set $\mathcal{C}$ and the input-to-state safe set $\mathcal{C}_d$ is shown in Figure 1.

In [16], input-to-state safety is defined with respect to the space $\mathbb{R}^n$. In this study, we extend it to Banach space $\mathcal{B}^\tau$ and the corresponding definition of input-to-state safety is given as follows.

Definition 5 (Input-to-state safety). Let $\mathcal{C}\subset\mathcal{B}^\tau$ be a set characterized by (5)–(7) for a continuous and differentiable functional $\mathcal{H}:\mathcal{B}^\tau\rightarrow\mathbb{R}$, if there exist $\beta\in\mathcal{K}_{[0,a)}$ with $\lim_{r\rightarrow a}\beta(r)=b$ and a constant $\bar{d}\in[0,a)$, such that $\mathcal{C}_d$ characterized by (14)–(16) is forward invariant for all d with $\|d\|_\infty\leqslant\bar{d}$, then the set $\mathcal{C}$ is an ISSf set.

According to Definition 5, we can find that the set $\mathcal{C}$ is input-to-state safe if and only if $\mathcal{C}_d$ is forward invariant. Therefore, let $\mathcal{C}_d$ be the safe set, we can get the corresponding set $\mathcal{C}$ according to the maximum disturbance value. We use the following example to enhance the understanding of input-to-state safety.

Example 1. Consider the following time-delay system with nonlinear dynamics:

$$\dot{x}(t)=-\frac{1}{2}x^3(t)-\frac{1}{4}x^3(t-\tau)+x(t)u(t), \tag{17}$$

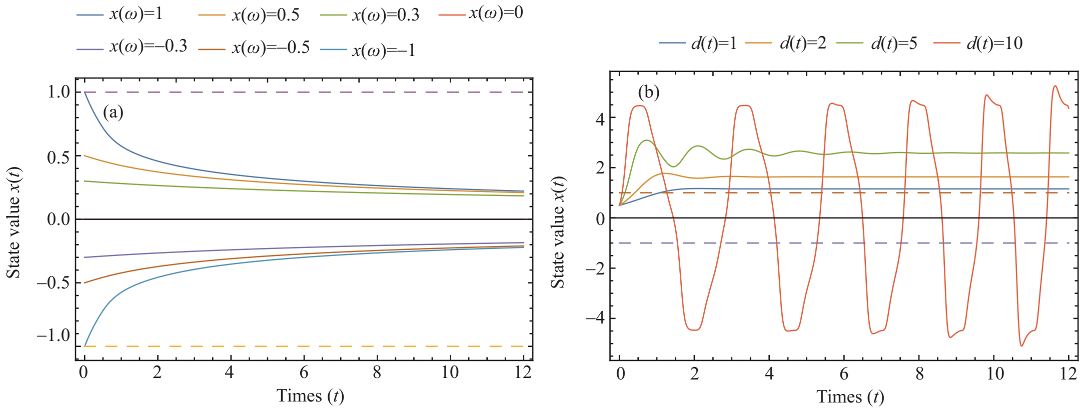

Figure 2 (Color online) (a) State evolution of the system for different initial conditions $x(\omega)$. The dashed lines correspond to $x=-1$ and $x=1$, the boundaries of the safe set. (b) State evolution of the system for different disturbances d. The dashed lines correspond to $x=-1$ and $x=1$, the boundaries of the safe set.

where $x\in\mathbb{R}$ and $u(\cdot):\mathbb{R}_{\geqslant 0}\to U\subset\mathbb{R}$.

First, our goal here is to find a barrier functional by the controller $u(t)=k(x(t))\equiv 0$ and show that a safe set can be constructed when the time delay τ is small enough. According to [45], the system is asymptotically delay-independently stable and has one equilibrium $x_t(\omega)=x(t+\omega)=x^*$, $\omega\in[-\tau,0]$, $t\geqslant 0$. Consequently, there exists an attraction region [40], which is a safe subset of the state space in which an equilibrium point is rendered to be asymptotically stable by the given controller. In this example the equilibrium is $x^*=0$, then a safe set around $x^*=0$ can be constructed and we set the safe set to be $[-1,1]$. We define the control barrier functional as

$$\mathcal{H}(\psi)=1-\psi^4(0).$$

Given the above barrier functional, we instantiate the parameter as $\tau=1/2$ and choose $\alpha(\mathcal{H})=\beta\mathcal{H}$ with $\beta\geqslant 0$ as the class $\mathcal{K}$ function in (11). Then the following equation can be obtained:

$$\begin{aligned}\dot{\mathcal{H}}(\psi)+\beta\mathcal{H}(\psi)&=2\psi^6(0)+\psi^3(0)\psi^3\left(-\frac{1}{2}\right)+\beta(1-\psi^4(0))\\&\geqslant\psi^4(0)(2\psi^2(0)-\beta)+\psi^3(0)\psi^3\left(-\frac{1}{2}\right)+\beta\\&\geqslant\left(\psi^3(0)+\frac{1}{2}\psi^3\left(-\frac{1}{2}\right)\right)^2+\psi^6(0)-\frac{1}{4}\psi^6\left(-\frac{1}{2}\right)+\beta.\end{aligned}$$

If we choose a small enough β, the following equation holds:

$$\dot{\mathcal{H}}(\psi)+\beta\mathcal{H}(\psi)\geqslant 0.$$

That is, condition (11) holds. According to Theorem 1, the system is safe. Trajectories with different initial conditions $x(\omega)\equiv 1$, 0.5 ,0.3, 0, -0.3, -0.5, -1 for $\omega\in[-1/2,0]$ are shown in Figure 2.

According to the above analysis, we know that the controller $k(x(t))\equiv 0$ can guarantee the safety of system (17). Now, under the same conditions, we consider the presence of disturbance d, i.e., the system becomes

$$\dot{x}(t)=-\frac{1}{2}x^3(t)-\frac{1}{4}x^3(t-\tau)+x(t)(u(t)+d). \tag{18}$$

We choose $k(x(t))\equiv 0$ and $\alpha(\mathcal{H})=\beta\mathcal{H}$ with $\beta\geqslant 0$ as the class $\mathcal{K}$ function in (11). Hence, we get

$$\begin{aligned}\dot{\mathcal{H}}(\psi)+\beta\mathcal{H}(\psi)&=2\psi^6(0)+\psi^3(0)\psi^3\left(-\frac{1}{2}\right)-4\psi^4(0)d+\beta(1-\psi^4(0))\\&\geqslant\psi^4(0)(2\psi^2(0)-\beta-4d)+\psi^3(0)\psi^3\left(-\frac{1}{2}\right).\end{aligned} \tag{19}$$

According to (19), it is easy to find that condition (11) may not hold when d becomes larger. We choose the initial condition $x(\omega)\equiv 0.5$ for $\omega\in[-1/2,0]$, and use different values on $d(\cdot)\equiv 1,2,5,10$, the resulting trajectories are presented in Figure 2(b). Obviously, some trajectories leave the specified safe set $[-1,1]$ in finite time, implying that the system is not safe. Also, it is observed that when the disturbance reaches a certain limit, the resulting trajectories do not even converge. That is, the controller $k(x(t))\equiv 0$ cannot always guarantee the safety of the system subject to disturbances.

5.2 The input-to-state safe control barrier functionals

Base on the definition of input-to-state safety, we provide an approach to guarantee the safety of DDEs with disturbances by input-to-state safe barrier functionals (ISSf-BFs) and ISSf-CBFs in this subsection. Before defining ISSf-BFs, we first introduce a constant e, which is useful for defining comparison function, as follows:

$$e=-\lim_{r\to -b}\alpha(r).$$

Definition 6 (ISSf-BFs)**.** For the time-delay system (13), let $\mathcal{C}$ be a set defined as (5)–(7) with a continuous and differentiable functional $\mathcal{H}:\mathcal{B}^{\tau}\to\mathbb{R}$. If there exist a function $\varepsilon\in\mathcal{K}_{[0,a)}$ with $\lim_{r\to a}\varepsilon(r)=e$, a function $\alpha\in\mathcal{K}_{(-b,c)}$, and $\bar{d}\in[0,a)$, such that $\forall x_t\in\mathcal{C}$, $\forall d(\cdot):\mathbb{R}_{\geqslant 0}\to\mathbb{R}^m$ satisfying $\|d\|_\infty\leqslant\bar{d}$,

$$\dot{H}(x_t)\geqslant-\alpha(\mathcal{H}(x_t))-\varepsilon(\|d\|_\infty),\tag{20}$$

then we say $\mathcal{H}$ is an input-to-state safe barrier functional.

Theorem 2 can guarantee the safety of time-delay systems in the presence of disturbances.

Theorem 2. For the time-delay system (13), let $\mathcal{C}\subset\mathcal{B}^{\tau}$ be a set defined by (5)–(7) with a continuous and differentiable functionals $\mathcal{H}:\mathcal{B}^{\tau}\to\mathbb{R}$, $\mathcal{C}_d$ characterized by (14)–(16) for an $\beta\in\mathcal{K}_{[0,a)}$ with $\lim_{r\to a}\beta(a)=b$ and $\bar{d}\in[0,a)$. If $\mathcal{H}$ is an ISSf-BF, then $\mathcal{C}$ is input-to-state safe.

Proof. We just need to prove $\mathcal{C}_d$ is forward invariant. According to the definition of $\mathcal{C}_d$, we get a new functional

$$\zeta(x_t,d)=\mathcal{H}(x_t)+\beta(\|d\|_\infty).$$

We can get the following equation from (20) for $\mathcal{H}$, which is an ISSf-BF

$$\begin{aligned}\dot{\zeta}(x_t,d)=\dot{\mathcal{H}}(x_t)&\geqslant-\alpha(\mathcal{H}(x_t))-\varepsilon(\|d\|_\infty)\\&=-\alpha(\zeta(x_t,d)-\beta(\|d\|_\infty))-\varepsilon(\|d\|_\infty).\end{aligned}\tag{21}$$

Consider the boundary $\partial\mathcal{C}_d$. Since $\zeta(x_t,d)=0$ for $x_t\in\partial\mathcal{C}_d$, Eq. (21) can be reduced as

$$\dot{\zeta}(x_t,d)\geqslant-\alpha(-\beta(\|d\|_\infty))-\varepsilon(\|d\|_\infty).$$

Setting $r=\beta(\|d\|_\infty)$ and defining $\rho(r):=-\alpha(-r)$, we have that for all $r_1,r_2\in\mathbb{R}_{\geqslant 0}$ and $r_1>r_2$ implies that $-\alpha(-r_1)>-\alpha(-r_2)$, implying that $\rho(r_1)>\rho(r_2)$. Thus, if $r<b$, ρ is a class $\mathcal{K}$ function. Consequently, by choosing $\beta=\rho^{-1}\circ\varepsilon$, it follows that for any $\bar{d}\in[0,a)$,

$$\rho^{-1}\circ\varepsilon(\bar{d})<b,$$

which further implies $r<b$, thus

$$\dot{\zeta}(x_t,d)\geqslant\varepsilon(\|d\|_\infty)-\varepsilon(\|d\|_\infty)\geqslant 0.\tag{22}$$

The result follows immediately as $\mathcal{C}_d$ is forward invariant by (22).

Theorem 2 shows that ISSf-BFs can guarantee the input-to-state safety of time-delay systems under disturbances. In order to deal with control input, we give the definition of ISSf-CBFs in the following and demonstrate its role in safety guarantee.

Definition 7 (ISSf-CBFs). For the time-delay system (13), let $\mathcal{C}$ be a set defined by (5)–(7) with a continuous and differentiable functional $\mathcal{H}:\mathcal{B}^{\tau}\to\mathbb{R}$. If there exist a $\varepsilon\in\mathcal{K}_{[0,a)}$ with $\lim_{r\to a}\varepsilon(r)=e$, an $\alpha\in\mathcal{K}_{(-b,c)}$, and a constant $\bar{d}\in[0,a)$ such that for $x_t\in\mathcal{C}$ and $d(\cdot):\mathbb{R}_{\geqslant 0}\to\mathbb{R}^m$ satisfying $\|d\|_\infty\leqslant\bar{d}$,

$$\sup_{u(t)\in U}[\dot{\mathcal{H}}(x_t)]\geqslant-\alpha(\mathcal{H}(x_t))-\varepsilon(\|d\|_\infty),\tag{23}$$

then we say $\mathcal{H}$ is an input-to-state safe control barrier functional.

Inspired by the controller construction in [44], we construct our input-to-state safe controller in a similar way. For a safekeeping controller $k(x(t))$, we propose the input-to-state safe controller as follows:

$$u(t) = k(x(t)) + \mathcal{H}_{\mathcal{G}}(x_t), \tag{24}$$

where $\mathcal{H}_{\mathcal{G}}(x_t)$ denotes the derivative of $\mathcal{H}$ with respect to $\mathcal{G}$. A theorem is given below based on the input-to-state safe controller (24). A new ISSf-CBF, which can guarantee that the set $\mathcal{C}$ is input-to-state safe, is defined in Theorem 3.

Theorem 3. Given time-delay system (13), a set $\mathcal{C} \subset \mathcal{B}^{\tau}$ defined by (5)–(7) with a continuous and differentiable functional $\mathcal{H} : \mathcal{B}^{\tau} \to \mathbb{R}$, if $\mathcal{H}$ satisfies

$$\sup_{u(t)\in U} [\mathcal{H}_{\mathcal{F}}(x_t) + \mathcal{H}_{\mathcal{G}}(x_t)u(t) - \mathcal{H}_{\mathcal{G}}(x_t)\mathcal{H}_{\mathcal{G}}(x_t)^{\mathrm{T}}] \geqslant -\alpha(\mathcal{H}(x_t)),\ \forall x_t \in \mathcal{C}, \tag{25}$$

for some $\alpha \in \mathcal{K}_{(-b,c)}$, then $\mathcal{H}$ is an input-to-state safe control barrier functional.

Proof. According to (25), we have

$$\dot{\mathcal{H}}(x_t) \geqslant -\alpha(\mathcal{H}(x_t)) + \mathcal{H}_{\mathcal{G}}(x_t)\mathcal{H}_{\mathcal{G}}(x_t)^{\mathrm{T}} + \mathcal{H}_{\mathcal{G}}(x_t)d(t).$$

Since $\mathcal{H}_{\mathcal{G}}(x_t)\mathcal{H}_{\mathcal{G}}(x_t)^{\mathrm{T}} = |\mathcal{H}_{\mathcal{G}}(x_t)|^2$, we have

$$\dot{\mathcal{H}}(x_t) \geqslant -\alpha(\mathcal{H}(x_t)) + |\mathcal{H}_{\mathcal{G}}(x_t)|^2 - |\mathcal{H}_{\mathcal{G}}(x_t)|\|d\|_{\infty}. \tag{26}$$

Implying that

$$\begin{aligned}\dot{\mathcal{H}}(x_t) &\geqslant -\alpha(\mathcal{H}(x_t)) + \left(|\mathcal{H}_{\mathcal{G}}(x_t)| - \frac{\|d\|_{\infty}}{2}\right)^2 - \frac{\|d\|_{\infty}^2}{4} \\ &\geqslant -\alpha(\mathcal{H}(x_t)) - \frac{\|d\|_{\infty}^2}{4},\end{aligned}$$

which has the same form as (23). Thus, $\mathcal{H}$ is a valid ISSf-CBF.

Theorem 3 shows that an input-to-state safe controller can guarantee the safety of time-delay systems in the presence of disturbances. Similar to the CBF condition (11), when $\mathcal{H}_{\mathcal{G}}(x_t) = 0$, Theorem 3 can only verify whether $k(x(t)) \equiv 0$ is a safe controller. In the following, we use an example to enhance the understanding of input-to-sate safe controllers.

Example 2. Consider the time-delay system with $\tau = 1/2$ in Example 1. As discussed in Example 1, the safekeeping controller $k(x(t)) \equiv 0$ can guarantee the safety of system (17) in the absence of disturbances. However, if system (17) is subject to disturbances such as $d(\cdot) \equiv 1, 2, 5$, i.e., system (18), the controller cannot ensure the safety of system (18).

Now we apply the following input-to-state safe controller to system (18):

$$u(t) = k(x(t)) + \mathcal{H}_{\mathcal{G}}(x_t)^{\mathrm{T}} = -4x^4(t). \tag{27}$$

The system driven by the controller (27) will evolve in the safe set subject to certain disturbances such as $d(\cdot) \equiv 1, 2, 3, 5$. Some trajectories are displayed in Figure 3.

6 Implementation and experiments

In this section, we first present our algorithm for synthesizing input-to-state safe controllers in Algorithm 1. If there are no disturbances in the system (line 2), the controller given by Theorem 1 (line 1) is safekeeping, so Algorithm 1 returns this controller directly. Otherwise, our algorithm gives an input-to-state safe controller based on Theorem 3 (line 5). Algorithm 1 shows that safekeeping controllers can be synthesized by solving constraint (11), and the input-to-state safe controllers, which ensure the safety of the considered system in the presence of disturbances, can be easily obtained based on the safekeeping controller. However, the generation of $k(x(t))$ is still a challenging problem, which will be investigated in our future work. The present work is based on the condition that $k(x(t))$ can be automatically generated or already exists.

Now we use three examples to demonstrate our method.

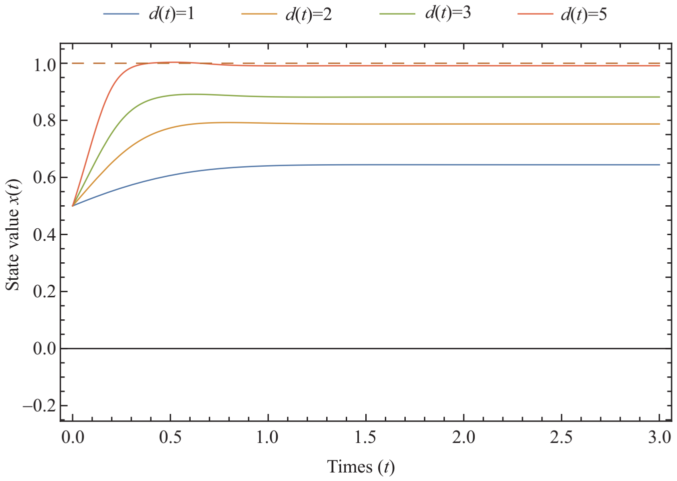

Figure 3 (Color online) State evolution of the system for different disturbances when applying the input-to-state safe controller (27). The dashed lines correspond to $x=-1$ and $x=1$, the boundary of the safe set.

Algorithm 1 Input-to-state safe controller

```
Require: Time-delay system $S$; barrier functional $\mathcal{H}$; disturbance $d$.
Ensure: Control input $u(t)$.
1: Synthesize $k(x(t))$ from the control barrier functional condition: $\sup_{k(x(t))\in U}[\dot{\mathcal{H}}(x_t)] \geqslant -\alpha(\mathcal{H}(x_t))$;
2: if $d \equiv 0$ then
3:     $u(t) = k(x(t))$;
4: else
5:     $u(t) = k(x(t)) + \mathcal{H}_{\mathcal{G}}(x_t)^{\mathrm{T}}$;
6: end if
7: return $u(t)$.
```

Example 3. Consider the following dynamical system, adapted from [45]:

$$\dot{x}(t) = -x(t) - \frac{1}{2}x(t-\tau) + x(t)(u(t)+d(t)), \tag{28}$$

where $x \in \mathbb{R}^n$, $u(\cdot): \mathbb{R}_{\geqslant 0} \to U$, $d \in [0,2]$ is a constant disturbance. The safe set is $[-1,1]$. In this case, we choose the barrier functional as

$$\mathcal{H}(\psi) = 1 - \psi^2(0). \tag{29}$$

Given the barrier functional (29), we discuss two cases with and without disturbances in the following:

(a) Without disturbances, i.e., $d=0$. We choose $\alpha(\mathcal{H}) = \beta\mathcal{H}$ with $\beta > 0$ as the class $\mathcal{K}$ function in (11). Then let $\tau = 1/2$ and $k(x(t)) = 0$, we get

$$\begin{aligned}\dot{\mathcal{H}}(\psi) + \beta\mathcal{H}(\psi) &= 2\psi^2(0) + \psi(0)\psi\left(-\frac{1}{2}\right) + \beta(1-\psi^2(0))\\ &\geqslant (2-\beta)\psi^2(0) + \psi(0)\psi\left(-\frac{1}{2}\right) + \beta.\end{aligned}$$

When we choose a small β, the following equation holds:

$$\dot{\mathcal{H}}(\psi) + \beta\mathcal{H}(\psi) \geqslant 0.$$

Thus $k(x(t)) \equiv 0$ satisfies the control barrier functional condition, the set $[-1,1]$ is safe. Algorithm 1 returns $u \equiv 0$.

(b) With disturbances, i.e., $d \neq 0$. Different values on d are taken, i.e., $d = 0.5,\ 1,\ 1.5,\ 2$, to run Algorithm 1. Taking $\alpha(\mathcal{H}) = \beta\mathcal{H}$ with $\beta > 0$ as the class $\mathcal{K}$ function in (11) and $k(x(t)) \equiv 0$, we get

$$\dot{\mathcal{H}}(\psi) + \beta\mathcal{H}(\psi) = 2\psi^2(0) + \psi(0)\psi\left(-\frac{1}{2}\right) - 2\psi^2(0)d + \beta(1-\psi^2(0))$$

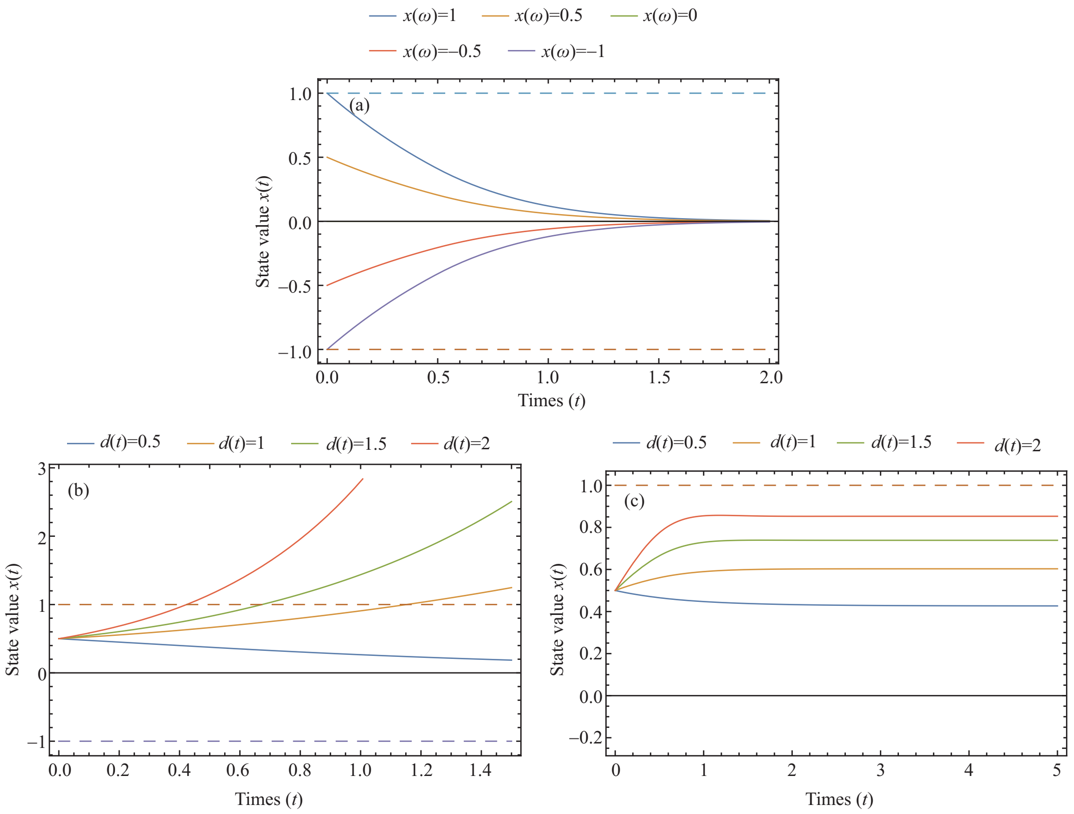

Figure 4 (Color online) (a) Trajectories of the system for different initial functions. The dashed lines correspond to $x = -1$ and $x = 1$, representing the boundaries of the safe set. (b) Trajectories of the system for different disturbances. The dashed lines correspond to $x = -1$ and $x = 1$, the boundaries of the safe set. (c) Trajectories of the system for different disturbances with the input-to-state safe controller. The dashed lines correspond to $x = -1$ and $x = 1$, the boundaries of the safe region.

$$\geqslant (2-\beta-d)\psi^2(0)+\psi(0)\psi\left(-\frac{1}{2}\right)+\beta.$$

We can find when the disturbance d reaches a certain limit, condition (11) will not hold, so the system becomes unsafe. As shown in Figure 4(b), the system is safe when the disturbance d is equal to 0.5, but when the disturbance d is 1, 1.5 or 2, the system is not safe.

Now we use the following input-to-state safe controller as in (24), we get

$$u(t) = k(x(t)) + \mathcal{H}_{\mathcal{G}}(x_t) = -2x^2(t).$$

By applying the input-to-state safe controller to system (28), the input-to-state safe controller can ensure system (28) safe under small disturbances according to Theorem 3. Some safe trajectories are demonstrated in Figure 4(c) when the disturbance d takes 1, 1.5, and 2, respectively.

Example 4 (Population dynamics)**.** Let us consider a population related dynamical system adapted from [46], given by

$$\dot{q}(t) = \lambda[1-q(t-\tau)/M]q(t),\ t \geqslant 0.$$

This equation is used to simulate the change of the number of individuals in a single population in nature. Due to restrictions such as minimum breeding ages or limited resources, the average growth rate $\dot{q}(t)/q(t) = \lambda[1-q(t-\tau)/M]$ of the population relies on the size of the population in the past τ time units, because individual growth and resource recovery require a certain amount of time. If we set $x(t) = q(t)/M$ and adjust the time scale at the same time, we can get the following time-delay system as in [47]:

$$\dot{x}(t) = x(t)[1-x(t-\tau)] - (u(t)+d(t)),\ t \geqslant 0,$$

where $x \in \mathbb{R}$ represents the individual number, $u : \mathbb{R}_{\geqslant 0} \to U$ denotes the capture behavior, $d : \mathbb{R}_{\geqslant 0} \to \mathbb{R}$ denotes the constant disturbance. The goal is to keep the number of individuals within $[0.5, 1.6]$. We take a barrier functional as

$$H(\psi) = 0.55^2 - (\psi(0) - 1.05)^2.$$

Given this barrier functional, we discuss two cases involving the absence and presence of disturbances in the following:

(a) Without disturbances, i.e., $d = 0$. We choose $\alpha(\mathcal{H}) = \beta\mathcal{H}$ with $\beta > 0$ as the class $\mathcal{K}$ function in (11). Instantiating $\tau = 1.5$, we get

$$\begin{aligned}&\dot{\mathcal{H}}(\psi) + \beta H(\psi)\\ &= -2(\psi(0) - 1.05)\psi(0)(1 - \psi(-1.5)) + 2(\psi(0) - 1.05)u(t) + \beta(0.55^2 - (\psi(0) - 1.05)^2) \geqslant 0.\end{aligned} \tag{30}$$

If we choose $u(t) = k(x(t)) \equiv 0$, there exists a small β such that condition (30) holds, so $k(x(t)) \equiv 0$ satisfies the control barrier functional condition, the set $[0.5, 1.6]$ is safe. Algorithm 1 returns $u \equiv 0$. As shown in Figure 5(a), the system always evolves within the safe set.

(b) With disturbances: we take different values on d, i.e., $d = -0.5, -1, -1.5$, to run Algorithm 1, respectively. Choosing $\alpha(\mathcal{H}) = \beta\mathcal{H}$ with $\beta > 0$ as the class $\mathcal{K}$ function in (11) and assuming $k(x(t)) \equiv 0$, we have

$$\begin{aligned}&\dot{\mathcal{H}}(\psi) + \beta H(\psi)\\ &= -2(\psi(0) - 1.05)\psi(0)(1 - \psi(-1.5)) + 2(\psi(0) - 1.05)d + \beta(0.55^2 - (\psi(0) - 1.05)^2) \geqslant 0.\end{aligned} \tag{31}$$

If the disturbance d is large, the condition (31) cannot hold. As shown in Figure 5(b), the system cannot stay within the safe set for all time when $d = -0.5, -1, -1.5$.

Now by employing the following input-to-state safe controller as in (24):

$$u(t) = k(x(t)) + \mathcal{H}_{\mathcal{G}}(x_t) = 2(x(t) - 1.05).$$

We can conclude that the system is safe under small disturbances according to Theorem 3. Figure 5 shows some safe trajectories when $d = -0.5, -1, -1.5$.

Example 5 (PD-controller)**.** The following linear PD-controller is taken from [29, 36], defined as

$$\begin{cases}\dot{x}(t) = s(t),\\ \dot{s}(t) = -a_1(x(t-\tau) - x^*) - a_2 s(t-\tau) + s(t)(u(t) + d(t)),\end{cases} \tag{32}$$

where x denotes the position and s is velocity of an autonomous vehicle, u represents the input to control speed, d represents the unknown disturbance, and the constant τ is the time delay resulting from sensing, transmission, computation, and actuation. The vehicle needs adjust its acceleration in the light of the distance between the current location and the reference location x^*. The parameters are instantiated as $a_1 = 2$, $a_2 = 3$, $x^* = 1$, and $\tau = 0.35$. The system modeled by (32) is then transformed into the following form with $\hat{x} = x - 1$:

$$\begin{cases}\dot{\hat{x}}(t) = s(t),\\ \dot{s}(t) = -2\hat{x}(t-\tau) - 3s(t-\tau) + s(t)(u(t) + d(t)).\end{cases} \tag{33}$$

Let $x_1 = \hat{x}$, $x_2 = s$, and $\mathcal{X} = \left[\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right]$, the system (33) can be rewritten as a dynamical system described by two-dimensional matrix as follows:

$$\dot{\mathcal{X}} = A_1\mathcal{X}(t) + A_2\mathcal{X}(t-\tau) + B\mathcal{X}(t)(u(t) + d(t)), \tag{34}$$

where A_1, A_2, B are as follows:

$$A_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \ A_2 = \begin{bmatrix} 0 & 0 \\ -2 & -3 \end{bmatrix}, \ B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

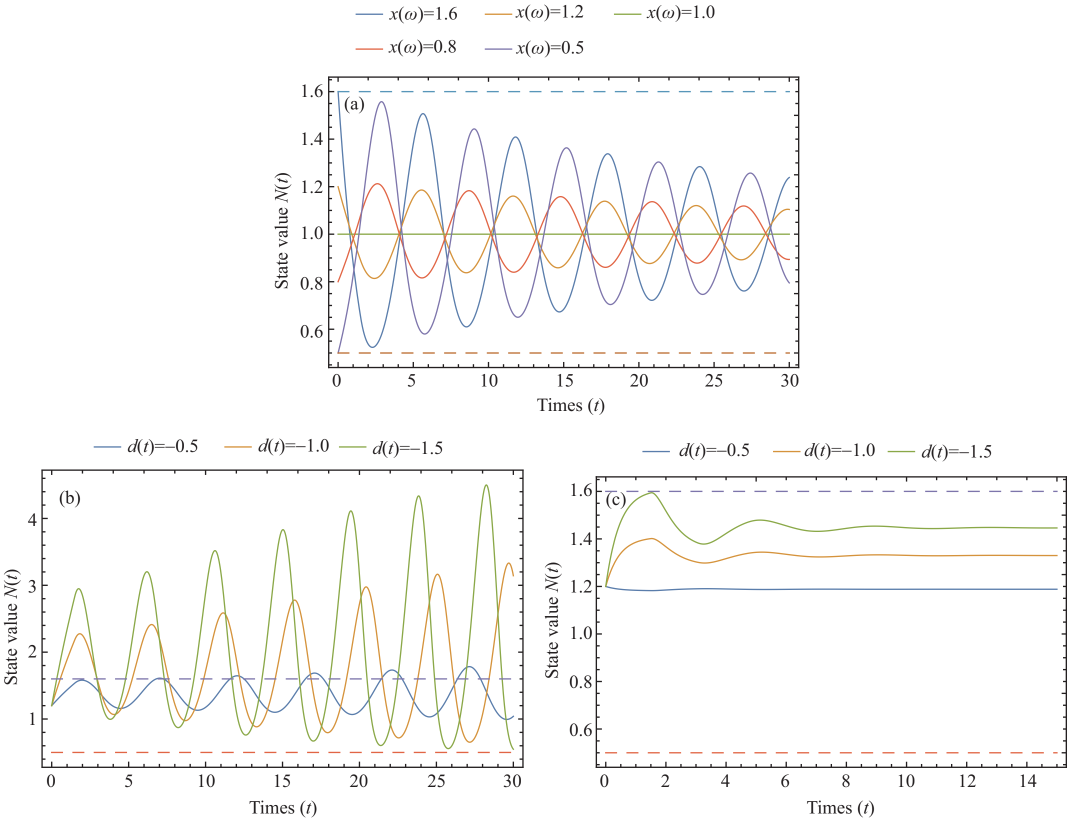

Figure 5 (Color online) (a) Trajectories of the system for different initial conditions. The dashed lines correspond to $x = 0.5$ and $x = 1.6$, the boundary of the safe set. (b) Trajectories of the system for different disturbances. The dashed lines correspond to $x = 0.5$ and $x = 1.6$, the boundary of the safe set. (c) Trajectories of the system for different disturbances with the input-to-state safe controller. The dashed lines correspond to $x = 0.5$ and $x = 1.6$, the boundary of the safe region.

The safe state set is $\mathcal{S} = \{(\hat{x}; s) \mid \hat{x} < 0.2, s < 0.4\}$ and the initial states set is $\mathcal{X} = [-0.1,\ 0.1] \times [0,\ 0.1]$. We choose the control barrier functional as

$$\mathcal{H}(\psi) = \begin{bmatrix} 0.2 \\ 0.4 \end{bmatrix} - \psi(0).$$

Given the barrier functional, we also discuss two cases, i.e., with and without disturbances:

(a) Without disturbances, i.e., $d = 0$. We set $u = 0$. As discussed in [29], the system has one equilibrium at $(0; 0)$ and is safe. By choosing $\alpha(\mathcal{H}) = \beta\mathcal{H}$ with $\beta > 0$ as the class $\mathcal{K}$ function in (11), we can also easily find that the following equation holds:

$$\dot{\mathcal{H}}(\psi) + \beta\mathcal{H}(\psi) \geqslant 0.$$

Therefore, $k(\mathcal{X}) \equiv 0$ is a safekeeping controller. Some trajectories of the system are displayed in Figure 6(a).

(b) With disturbances, i.e., $d \neq 0$. Consider the situation with disturbance, we take the following time-varying disturbance as the input of Algorithm 1.

$$d(t) = 1 + 0.2\sin(t).$$

Also, we display some trajectories of the system in Figure 6(b). Obviously, the system violates the safety constraint. That is, $k(\mathcal{X}) \equiv 0$ cannot guarantee the safety of the system.

By applying the following input-to-state safe controller to the system:

$$u(t) = k(\mathcal{X}(t)) + \mathcal{H}_{\mathcal{G}}(\phi) = -x_2(t).$$

Figure 6 displays some trajectories of this system driven by the new input-to-state safe controller, the input-to-state safe controller can ensure the safety of the system under small disturbances.

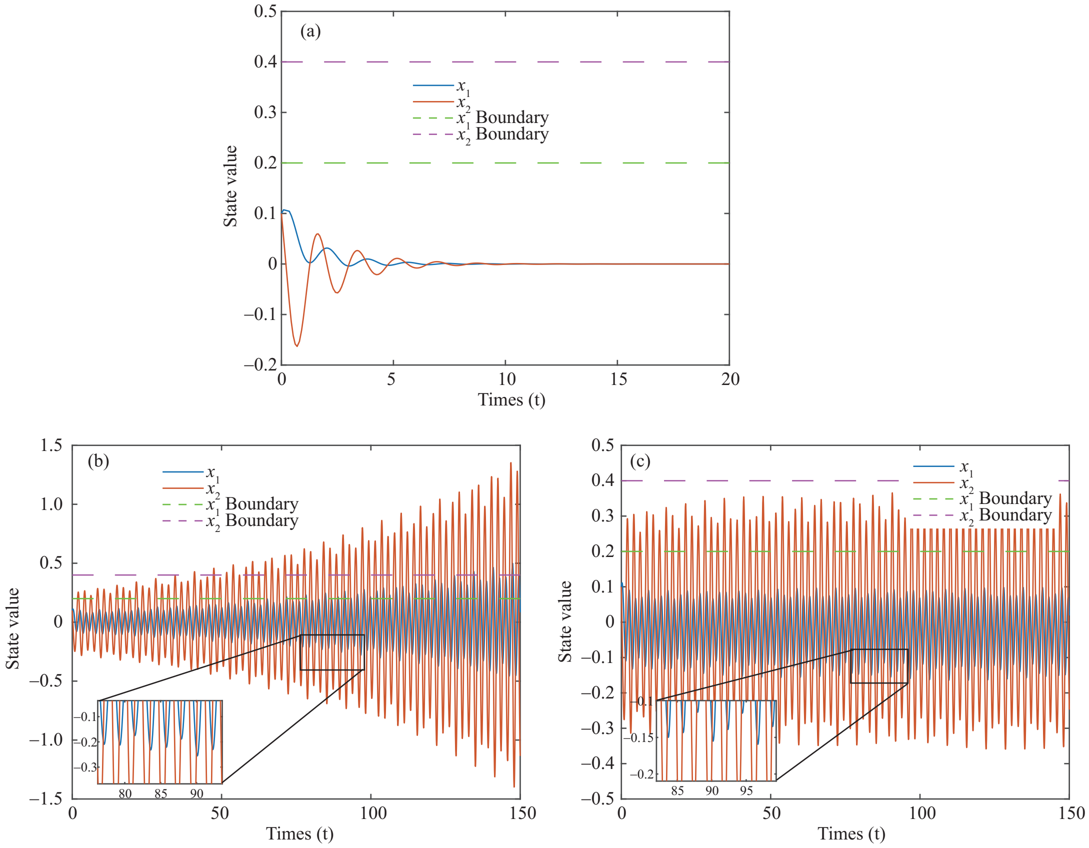

Figure 6 (Color online) (a) Trajectories of the system for initial conditions $x_1 = 0.1$, $x_2 = 0.1$. The dashed lines corresponding to $x = 0.2$ and $x = 0.4$ represent the safe boundaries of states x_1 and x_2, respectively. (b) Trajectories of the system for disturbance $d(t) = 1 + 0.2\sin(t)$. The dashed lines corresponding to $x = 0.2$ and $x = 0.4$ represent the safe boundaries of states x_1 and x_2, respectively. (c) Trajectories of the system for disturbance $d(t) = 1 + 0.2\sin(t)$ with the input-to-state safe controller. The dashed lines corresponding to $x = 0.2$ and $x = 0.4$ represent the safe boundaries of states x_1 and x_2, respectively.

7 Conclusion

In this paper, we investigated the safety verification for time-delay systems subject to control inputs and disturbances. We proposed ISSf-CBFs to guarantee the safety. Finally, the theoretical developments of our approach were demonstrated using three examples.

In the future, it deserves to investigate how to synthesize controllers for time-delay systems and extend our method to high order control barrier functionals to guarantee the safety of time-delay systems with a higher relative degree, as well as time-delay systems with frequency domains.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant Nos. 61625206, 61732001, 61836005, 61872341, 61972385). In addition, we thank Dr. Bai XUE for helpful discussions.

References

1 Chen T M, Sanchez-Aarnoutse J C, Buford J. Petri net modeling of cyber-physical attacks on smart grid. IEEE Trans Smart Grid, 2011, 2: 741–749
2 Jia D T, Lu K, Wang J, et al. A survey on platoon-based vehicular cyber-physical systems. IEEE Commun Surv Tut, 2016, 18: 263–284
3 Wang L, Törngren M, Onori M. Current status and advancement of cyber-physical systems in manufacturing. J Manuf Syst, 2015, 37: 517–527
4 Yang K. Delay Differential Equations: With Applications in Population Dynamics. Boston: Academic Press, 1993
5 Cooke K L. Stability analysis for a vector disease model. Rocky Mountain J Math, 1979, 9: 31–42
6 Datko R F. Theory of functional differential equations (Jack Hale). SIAM Rev, 1978, 20: 610–612
7 Stepan G. Delay effects in the human sensory system during balancing. Phil Trans R Soc A, 2009, 367: 1195–1212
8 Srikant R. The Mathematics of Internet Congestion Control. Boston: Springer, 2004
9 Shayer L P, Campbell S A. Stability, bifurcation, and multistability in a system of two coupled neurons with multiple time delays. SIAM J Appl Math, 2000, 61: 673–700
10 Myschkis A D. Lineare Differentialgleichungen MIT Nacheilendem Argument. Berlin: VEB Verlag, 1955
11 Bellman R E, Cooke K L. Differential-Difference Equations. California: RAND Corporation, 1963

12 Forbes J R. L2-gain and passivity techniques in nonlinear control, third edition [bookshelf]. IEEE Control Syst, 2017, 37: 75–76

13 Jayawardhana B, Logemann H, Ryan E P. The circle criterion and input-to-state stability. IEEE Control Syst, 2011, 31: 32–67

14 Prajna S, Jadbabaie A. Safety verification of hybrid systems using barrier certificates. In: Proceedings of International Workshop on Hybrid Systems: Computation and Control, 2004. 477–492

15 Ames A D, Grizzle J W, Tabuada P. Control barrier function based quadratic programs with application to adaptive cruise control. In: Proceedings of the 53rd IEEE Conference on Decision and Control, 2015. 6271–6278

16 Kolathaya S, Ames A D. Input-to-state safety with control barrier functions. IEEE Control Syst Lett, 2019, 3: 108–113

17 Prajna S, Jadbabaie A. Methods for safety verification of time-delay systems. In: Proceedings of the 44th IEEE Conference on Decision and Control, 2005. 4348–4353

18 Orosz G, Ames A D. Safety functionals for time delay systems. In: Proceedings of American Control Conference, 2019. 4374–4379

19 Wang X, Chiang H D, Wang J, et al. Long-term stability analysis of power systems with wind power based on stochastic differential equations: model development and foundations. IEEE Trans Sustain Energy, 2015, 6: 1534–1542

20 Hoogendoorn S P, Bovy P H L. Pedestrian route-choice and activity scheduling theory and models. Transp Res Part B-Meth, 2004, 38: 169–190

21 Black F, Scholes M. The pricing of options and corporate liabilities. J Political Econ, 1973, 81: 637–654

22 Panik M J. Stochastic Differential Equations: An Introduction with Applications in Population Dynamics Modeling. Hoboken: Wiley, 2017

23 Fränzle M, Chen M, Kröger P. In memory of Oded Maler. ACM SIGLOG New, 2019, 6: 19–39

24 Kong H, He F, Song X Y, et al. Exponential-condition-based barrier certificate generation for safety verification of hybrid systems. In: Proceedings of International Conference on Computer Aided Verification, 2013. 242–257

25 Zeng X, Lin W, Yang Z F, et al. Darboux-type barrier certificates for safety verification of nonlinear hybrid systems. In: Proceedings of the 13th International Conference on Embedded Software, 2016. 1–10

26 Dai L Y, Gan T, Xia B C, et al. Barrier certificates revisited. J Symb Comput, 2017, 80: 62–86

27 Sogokon A, Ghorbal K, Tan Y K, et al. Vector barrier certificates and comparison systems. In: Proceedings of International Symposium on Formal Methods, 2018. 418–437

28 Liu J, Zhan N J, Zhao H J. Computing semi-algebraic invariants for polynomial dynamical systems. In: Proceedings of the 9th ACM International Conference on Embedded Software, 2011. 97–106

29 Feng S H, Chen M S, Zhan N J, et al. Taming delays in dynamical systems. In: Proceedings of the 31st International Conference on Computer-Aided Verification, Springer, 2019. 650–669

30 Pola G, Pepe P, di Benedetto M D, et al. Symbolic models for nonlinear time-delay systems using approximate bisimulations. Syst Control Lett, 2010, 59: 365–373

31 Pola G, Pepe P, di Benedetto M D. Symbolic models for time-varying time-delay systems via alternating approximate bisimulation. Int J Robust Nonlinear Control, 2015, 25: 2328–2347

32 Huang Z Q, Fan C C, Mitra S. Bounded invariant verification for time-delayed nonlinear networked dynamical systems. Nonlinear Anal-Hybrid Syst, 2017, 23: 211–229

33 Xue B, Mosaad P N, Fränzle M, et al. Safe over- and under-approximation of reachable sets for delay differential equations. In: Proceedings of International Conference on Formal Modeling and Analysis of Timed Systems, 2017. 281–299

34 Xue B, Wang Q Y, Feng S H, et al. Over- and underapproximating reach sets for perturbed delay differential equations. IEEE Trans Autom Control, 2021, 66: 283–290

35 Xue B, She Z K, Easwaran A. Under-approximating backward reachable sets by polytopes. In: Proceedings of International Conference on Computer Aided Verification, 2016. 457–476

36 Goubault E, Putot S, Sahlmann L. Inner and outer approximating flowpipes for delay differential equations. In: Proceedings of International Conference on Computer Aided Verification, 2018. 523–541

37 Zou L, Fränzle M, Zhan N J, et al. Automatic stability and safety verification for delay differential equations. In: Proceedings of International Conference on Computer Aided Verification, 2015. 338–355

38 Zuo Z Q, Ho D W C, Wang Y J. Reachable set bounding for delayed systems with polytopic uncertainties: the maximal Lyapunov-Krasovskii functional approach. Automatica, 2010, 46: 949–952

39 Blake W K. Mechanics of Flow-Induced Sound and Vibration. Orlando: Academic Press, 1986

40 Khalil H K. Nonlinear Systems. Englewood Cliffs: Prentice Hall, 2002

41 Teel A R, Praly L. A smooth Lyapunov function from a class-$\mathcal{KL}$ estimate involving two positive semidefinite functions. ESAIM-COCV, 2000, 5: 313–367

42 Romdlony M Z, Jayawardhana B. Robustness analysis of systems' safety through a new notion of input-to-state safety. Int J Robust Nonlinear Control, 2019, 29: 2125–2136

43 Romdlony M Z, Jayawardhana B. On the sufficient conditions for input-to-state safety. In: Proceedings of IEEE International Conference on Control & Automation, 2017. 170–173

44 Sontag E D. Smooth stabilization implies coprime factorization. IEEE Trans Autom Control, 1989, 34: 435–443

45 Hale J, Lunel S M V. Introduction to Functional Differential Equations. Berlin: Springer, 1993

46 Hutchinson G E. Circular causal systems in ecology. Ann NY Acad Sci, 1948, 50: 221–246

47 Liu C, Zhang Q L, Huang J. The dynamics and control of a harvested differential-algebraic prey-predator model. In: Proceedings of Chinese Control and Decision Conference (CCDC), 2011. 586–591