SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

February 2022, Vol. 65 122203:1–122203:14
https://doi.org/10.1007/s11432-020-3028-4

Safety criteria based on barrier function under the framework of boundedness for some dynamic systems

Zheren ZHU[1,2], Yi CHAI[1,2*], Zhimin YANG[3] & Chenghong HUANG[1,2]

[1]*State Key Laboratory of Power Transmission Equipment and System Security and New Technology, Chongqing University, Chongqing 400044, China;*
[2]*School of Automation, Chongqing University, Chongqing 400044, China;*
[3]*Chongqing High-Tech-Zone Feima Innovation Research Institute, Chongqing 400050, China*

Received 4 April 2020/Revised 5 June 2020/Accepted 14 July 2020/Published online 14 January 2022

Abstract Barrier functions have been reported to be useful in quantifying the safety of some dynamic systems. Usually, when using the barrier functions, we try to transform safety analysis issues of dynamic systems into a class of reachability issues from a safe set to an unsafe set. This article presents a novel sufficient safety criterion for some dynamic systems. The proposed criterion is based on the barrier function and works as long as the upper bound of the barrier function is kept non-positive. Further, we present a mathematical description of fault safety for some dynamic system that experienced a fault at a certain time and propose a corresponding fault safety criterion for the aforementioned system.

Keywords safety criteria, barrier function, fault safety, multi-hypersphere method, dynamic system

Citation Zhu Z R, Chai Y, Yang Z M, et al. Safety criteria based on barrier function under the framework of boundedness for some dynamic systems. Sci China Inf Sci, 2022, 65(2): 122203, https://doi.org/10.1007/s11432-020-3028-4

1 Introduction

It has been reported that functional structures of large-scale dynamic systems such as chemical process systems, manufacturing systems, and power systems are quite complex. The safety requirements for operation of these systems are strict and involve a high energy, high temperature, high voltage, high speed, and other characteristics. For phases of some energy-intensive operations, if an abnormal operation state or system fault is not detected or handled in time, huge energy may be released quickly within a short time, resulting in an accident. Therefore, how to analyze, identify, and predict the operational safety of dynamic systems, especially the safety after a component-level or system-level fault taking place when the system is in service, has become one of the most popular research directions in the fields of mechanical engineering, electrical engineering, system science, management, control engineering, and some other disciplines.

There are roughly four methods for analyzing the operational safety of dynamic systems. The first is to establish safe evolution models by using inductive analysis, logical deduction, and then employ qualitative and quantitative analyses methods to calculate the probability of safety incidents taking place in the system. This approach has resulted in a variety of mature and practical methods [1, 2], for example, preliminary hazard analysis (PHA) [3], failure modes and effects analysis (FMEA) [4], fault tree analysis (FTA) [5], hazard and operability analysis (HAZOP) [6], cause-consequence analysis (CCA) [7], safety review analysis (SRA) [8], and human reliability analysis (HRA) [9]. The second approach is by performing operational safety analysis of complex systems based on safety risk states [10–18], which usually employs a stochastic process [13, 14], Petri net [15, 16], or Bayesian network [17, 18] to estimate safety risk associated with each state and state transition probability of each node of the system so as to perform dynamic safety analysis of the system. The third method [19] involves transforming operational

* Corresponding author (email: chaiyi@cqu.edu.cn)

safety analysis of the system into a transient stability judgment after the occurrence of some expected accidents, mainly by using energy functions, dynamic safety region, and the bifurcation analysis to perform safety analysis of the system. The last method can be referred to as operational safety analysis of dynamic systems based on barrier functions (BFs) or barrier certificates [20–34] presented in this paper. This method is inspired by the Lyapunov stability theory, which transforms safety analysis problems into reachability problems.

In the field of automation, stability, reliability, and safety are the most important operating characteristics. We turn the analysis problem of stability into a computable existence problem of the solutions [35–37]. The reliability analysis is transformed into estimation problems using statistical mathematics techniques such as degradation and life prediction [38,39]. Further, safety analysis methods, which reflect the operating state of the system, are initially based on reliability analysis approach, which can be used to determine safety states and the possibility of an accident by performing some calculations. However, the engineers want to obtain the actual value of inevitability to be or not to be, with values 0 and 1, respectively. Further, they proposed a computable method based on the descriptions of the dynamic equations. However, such methods directly convert safety analysis of the system into a stability analysis problem. In fact, safety and stability can be regarded as indeed two different sets, although their intersections are not empty. Fortunately, Prajna et al. [21,22] have made a major contribution by proposing the BFs. With such a method, we only need to find or prove whether there exists a barrier function satisfying some constraint conditions that can guarantee that the motion trajectory of the operation state will not intersect with the unsafe state set. Currently, there are two approaches to this method. One was created by Prajna et al. [21–26], and the second one was proposed by Ames et al. [27–34]. The former pays attention to both safe and unsafe sets, which does not establish or perfect the method of constructing the BFs through analytical approach yet, while the latter only needs to focus on one state set using forward invariant theory and is mainly used in safety control, which can be integrated with commonly used control algorithms. Presently, the two genres of methods that are commonly used are limited by the fact that it is difficult to accurately establish actual dynamic equations of dynamic systems, thus, making it hard to apply the method in analyzing the safety of practical complex systems.

With the growing advances in the field of sensing technology, the mapping of information world and the physical world is increasingly becoming complete and comprehensive. People can use big data and artificial intelligence technologies such as big data analysis and deep learning to build a dynamic model for actual physical objects with complete mapping. Therefore, we can acquire the solutions to problems that are difficult to solve using model-based safety analysis methods.

Inspired by the research results of Prajna et al. [21, 22], Kong et al. [23], and Wang et al. [24, 25], this study looked into sufficient safety criteria for some dynamic systems. Owing to the inevitable system operation fault, the operating state of a dynamic system may fluctuate, making it difficult for the barrier function to ensure monotonicity. Based on this consideration, this paper proposes a new kind of sufficient conditions for BF-based safety criteria, which can serve as an effective complement to the original theory. Further, the proposed novel kind of safety criteria can allow the monotonicity of the barrier function to fluctuate or change within an acceptable range. Our target is to continuously explore, extend, improve and perfect this theoretical system of safety analysis, judgment, and control based on BFs or barrier certificates, which rely on equations of dynamic systems, state sets, and scalar functions used for multidimensional projection transformations denoted as $B(x)$.

There are six sections in this article. Section 1 is the introduction part, which briefly presents the significance of this research, background, and current situation. Section 2 discusses the system's operational safety and proposes its mathematical representation. Section 3 presents sufficient safety criteria based on BFs. Further, Section 4 presents how to construct BFs. We present some examples of simulation verification of the proposed method in Section 5. Section 6 presents a summary of the work.

2 System operational safety and its mathematical description

In essence, operational safety refers to the ability or characteristic of a dynamic system that ensures that the system does not experience systemic equipment damage, environmental damage, casualties, and property damage, because of dangerous factors such as defects, malfunctions, and operating mistakes when the system is in operation. Therefore, by analyzing and judging the operational safety of the system, we can conclude that a certain amount of conservative margin is needed to ensure that there is relatively sufficient time to implement safety control to prevent operational safety accidents when the system enters an unsafe state.

If we know the laws governing the operation of the system and its current faults, we hope to be able to predict the operating situation after the system encountered a fault, that is, whether the system will leave the current safe state and enter an unsafe state after a certain time. If such state prediction analysis can be achieved, the safety protection system can be implemented as soon as possible.

If we can use a mathematical approach to obtain some criteria or theorems for determining the operational safety level of the system, we can perform corresponding analysis or predictions of its operational safety. In this paper, we present such approaches for establishing sufficient safety criteria for classical dynamic systems.

A typical class of dynamic systems can be described as

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

where $f \in \mathbb{R}^m$ denotes an r-times continuously differentiable function $(1 < r \leqslant m)$ denoted by $C^r(\chi, \mathbb{R}^m)$. The system state can be expressed as $x(t) \in \chi \subseteq \mathbb{R}^m$, an unsafe set $\chi_u \subseteq \chi$, and the initial state set $\chi_0 \cap \chi_u = \emptyset$ $(\chi_0 \subseteq \chi)$.

We regard the system as being safe, i.e., there exists no motion $\phi(t; x_0, t_0)$ of the system (1) with $x_0 = x(t_0) \in \chi_0$, and $\phi(t; x_0, t_0) = x(t)$ that makes the set $\Omega = \{\phi(t; x_0, t_0), t \in [t_0, T]\}$ have $\Omega \cap \chi_u \neq \emptyset$, as $T \to +\infty$.

Remark 1. At the beginning [21], the T is both finite and positive. Fortunately, with Romdlony's work [20], the T can now approach infinity.

Definition 1 (fault safety)**.** For the system described as (1), at some time t_0^*, the system (1) has a fault $f_d(t)$ with $f_d \in C^r$ $(\mathbb{R}, \mathbb{R}^m)$, which results in a system described as

$$\dot{x}(t) = f(x(t)) + f_d(t). \tag{2}$$

The system (2) can be regarded as being safe if there is no motion $\phi(t; x_0^*, t_0^*)$ of the system (2) with $x_0^* \in \chi_0^* \subseteq \chi$, $\overset{*}{\chi_0} \cap \chi_u = \emptyset$, and $\phi(t; x_0^*, t_0^*) = x(t)$ that makes the set $\Omega = \{\phi(t; x_0^*, t_0^*), t \in [t_0^*, T]\}$ have $\Omega \cap \chi_u \neq \emptyset$ as $T \to +\infty$.

3 Sufficient safety criteria

The BF-based safety analysis method is deeply influenced by the Lyapunov stability theory. However, safety and stability are fundamentally different from each other. Stability usually focuses only on the results, namely, it is hoped that the operating state of the system will eventually reach dynamic stability or dynamic balance. The BF-based safety analysis method translates the safety analysis problem into a reachability problem irrespective of whether the trajectory of operating state of the system will or will not enter into an unsafe state. Therefore, safety of the system concerns both processes and results obtained under such constraints, which are needed to ensure that any operating state is outside the unsafe set, beginning from the initial state.

There is a system set up for the dynamic system described in (1). Suppose the barrier function $B(x) \in \mathbb{R}$ satisfies the condition $B(x) \leqslant 0$ for any state of the system in the safety permission set $S(\chi_0 \subseteq S \subseteq \mathbb{R}^m)$, and $B(x) \in \mathbb{R}$ can be found to satisfy $B(x) > 0$ for any state in the unsafe set χ_u, where there exists $S \cap \chi_u = \emptyset$. Therefore, we can determine whether there is no motion trajectory $\phi(t; x_0, t_0)$ of the system state that will enter into the unsafe set, beginning from the initial state. According to the above conditions, it is difficult to directly prove that $B(x) \leqslant 0$ is established for all system states through calculation. Therefore, we need to add sufficient conditions for computability constraints to the barrier function $B(x)$.

Scholars, such as Prajna et al. [21] and Kong et al. [23], have put forward corresponding sufficient conditions of $B(x)$, according to characteristics of their systems.

However, for some systems with regular or irregular fluctuations in their operating states or some systems with strict or non-strict periodic fault characteristics, such as intermittent faults, it would be difficult for the $B(x)$ to maintain monotonic reduction [21], or to satisfy the condition $\dot{B}(x(t)) < \lambda B(x(t))$ [23]. Based on such considerations, this paper proposes some sufficient conditions for the safety criteria of dynamic systems based on general BFs, and hopes to improve the universality of the method and provide a method for evaluating fault safety of the dynamic systems.

3.1 Sufficient condition

First, we need to prove some lemmas that will help prove the following theorems.

Lemma 1. A function $h(x)$ $(x \in \mathbb{R}, h(x) \in \mathbb{R})$, which is r-times $(r = 2)$ continuously differentiable, has n $(n \geqslant 2)$ extreme points in such a way that any two adjacent extreme points of $h(x)$ must be a local maximum value and a local minimum value.

Proof. (i) Assume x_i and x_{i+1} are two adjacent extreme points of $h(x)$ and that both of them are the local maximum points. Hence, we can get $h'(x_i) = h'(x_{i+1})$, and $h''(x_i) < 0$, $h''(x_{I+1}) < 0$. Therefore, $\exists$ α and β $(\alpha < \beta)$, s.t. $x \in (x_i, \alpha)$, $h'(x) < 0$ and $x \in (\beta, x_{i+1})$, $h'(x) > 0$. By applying root existence theorem [40], we can show that there is a γ $(\gamma \in [\alpha - \delta, \beta + \delta], \forall \delta > 0)$, which makes $h'(\gamma) = 0$, at least.

(a) γ is the only one. As $h(x) \in C^2$ $(\mathbb{R}, \mathbb{R})$, we can show that $x \in (\alpha, \gamma)$, $h'(x) \leqslant 0$, and $x \in (\gamma, \beta)$, $h'(x) \geqslant 0$. Thus, $\gamma \in (x_i, x_{i+1})$ is a local minimum point of $h(x)$.

(b) There is other one ξ_1 $(\xi_1 \in (\gamma, \beta))$, which makes $h'(\xi_1) = 0$. So, we can get one of γ and ξ_1, which is an extreme point.

(c) There are $\xi_1, \xi_2, \ldots, \xi_k$ $(\gamma < \xi_1 < \cdots < \xi_k < \beta)$, which result in $h'(\xi_j) = 0$ $(1 \leqslant j \leqslant k)$. By applying Rolle's mean value theorem [40], we can show that $\exists \lambda_1, \lambda_2, \ldots, \lambda_{k-1}$ $(\lambda_j \in (\xi_j, \xi_{j+1}))$, s.t. λ_j is a maximum or minimum of $h'(x)$ in (ξ_j, ξ_{j+1}). If all of λ_j are maximum, one of γ and ξ_1 is a local minimum point of $h(x)$. If all of λ_j are minimum, ξ_k is a local minimum point of $h(x)$. If some are maximum and others are minimum among all the λ_j, there is at least one local minimum point of $h(x)$. However, the assumption that x_i and x_{i+1} are two adjacent extreme points is not satisfied.

With (a), (b), and (c), the assumption fails.

(ii) Assume x_i and x_{i+1} are two adjacent extreme points of $h(x)$ and both of them are the local minimum points. It can also be shown that this assumption is also invalid.

With (i) and (ii), a function $h(x)$ $(x \in \mathbb{R}, h(x) \in \mathbb{R})$, which is r-times $(r = 2)$ continuously differentiable, has n $(n \geqslant 2)$ extreme points, in such a way that any two adjacent extreme points of $h(x)$ of the system must be a local maximum value and a local minimum value.

Lemma 2. There is a function $h(x) \in C^2(\mathbb{R}, \mathbb{R})$. Assume the maximum or the minimum point of $h(x)$ is x_0 $(x_0 \in (\alpha, \beta))$; then x_0 must be the local maximum or the local minimum point of $h(x)$.

Proof. (i) At first, let x_0 be the maximum of $h(x)$ in the domain (α, β). Therefore, we can get $h(x_1) \leqslant h(x_0)(x_1 \in (\alpha, x_0))$ and $h(x_2) \leqslant h(x_0)(x_2 \in (x_0, \beta))$. Thus, for $\forall \delta > 0$, $h'(x) \geqslant 0$ $(x \in (x_0 - \delta, x_0))$ and $h'(x) \leqslant 0$ $(x \in (x_0, x_0 + \delta))$. Therefore, x_0 is a local maximum of $h(x)$.

(ii) Let x_0 be the minimum of $h(x)$ in the domain (α, β). The same can be proved to show that x_0 is a local minimum of $h(x)$.

With (i) and (ii), the maximum or the minimum point x_0 $(x_0 \in (\alpha, \beta))$ of $h(x)$ $(h(x) \in C^2(\mathbb{R}, \mathbb{R}))$ must be the local maximum or the local minimum point of $h(x)$.

Lemma 3. A function $h(x)$ $(h(x) \in C^2(\mathbb{R}, \mathbb{R}))$ has n $(n \geqslant 2)$ extreme points. There are two adjacent extreme points α, β $(\alpha < \beta)$ such that for $\forall \theta$ $(\theta \in (\alpha, \beta))$, the condition $\min\{h(\alpha), h(\beta)\} < h(\theta) < \max\{h(\alpha), h(\beta)\}$ is always satisfied.

Proof. (i) Assume $\exists \theta$ $(\theta \in (\alpha, \beta))$, s.t. $h(\theta)$ is the maximum of $h(x)$ in domain (α, β). With Lemma 2, we can show that θ is a local maximum of $h(x)$. It does not correspond to the assumption that α, β are two adjacent extreme points, which implies that the assumption is invalid. Therefore, $\forall \theta$ $(\theta \in (\alpha, \beta))$, $h(\theta)$ is not the maximum of $h(x)$ in domain $[\alpha, \beta]$. This implies that $h(\theta) < \max\{h(\alpha), h(\beta)\}$.

(ii) Assume $\exists \theta$ $(\theta \in (\alpha, \beta))$, s.t. $h(\theta)$ is the minimum of $h(x)$ in domain (α, β). The same can be proved that $\min\{h(\alpha), h(\beta)\} < h(\theta)$.

With (i) and (ii), $\min\{h(\alpha), h(\beta)\} < h(\theta) < \max\{h(\alpha), h(\beta)\}$, $\forall \theta \in (\alpha, \beta)$.

Theorem 1 (sufficient condition)**.** The system described by Eq. (1) where $f(x)$ is $C^2(\chi, \mathbb{R}^m)$ and the initial state x_0 has $x_0 = x(t_0) \in \chi_0$ can be regarded as being safe if there is a barrier function $B(x)$ $(B(x) \in C^2(\chi))$ satisfying the following expressions:

$$B(x) < 0 \quad (\forall x \in \chi_0), \tag{3}$$

$$B(x) > 0 \quad (\forall x \in \chi_u), \tag{4}$$

$$\begin{aligned}&\frac{\partial B}{\partial x}(x(t_i))f(x(t_i))=0, \quad i=1,2,\ldots,n,\\&B(x(t_i))<0, \quad i=1,2,\ldots,n, \qquad (5)\\&\frac{\mathrm{d}^2B(x(t_n))}{\mathrm{d}t^2}<0,\\&\frac{\partial B}{\partial x}(x(t))f(x(t))<0 \quad (t>t_n), \qquad (6)\end{aligned}$$

where $\frac{\partial B}{\partial x}(x(t))f(x(t))=\frac{\mathrm{d}B(x(t))}{\mathrm{d}t}$, and n denotes a finite positive integer for condition (5).

Proof. (i) Assume $n=1$. It follows that $x(t_n)$ is only the extreme point of the $B(x(t))$, which is the only local maximum point of $B(x(t))$. As $B(x(t_n))<0$, there exists $B(x(t))<0$ $(t\geqslant t_0)$.

(ii) Assume t_i $(1\leqslant i\leqslant n-1)$ is not the extreme point of $B(x(t))$. It seems that $\frac{\mathrm{d}B(x(t_i))}{\mathrm{d}t}=0$ and $\frac{\mathrm{d}^2B(x(t_i))}{\mathrm{d}t^2}=0$ for every i $(1\leqslant i\leqslant n-1)$. Suppose that the function $\frac{\mathrm{d}B(x(t))}{\mathrm{d}t}$ crosses zero at $t=t_i$. It implies that t_i is an extreme point of the $B(x(t))$, which contradicts the assumption that it is not an extreme point. Thus, there must be $\mathrm{sgn}_{t\in(t_{i-1},t_i)}(\frac{\mathrm{d}B(x(t))}{\mathrm{d}t})=\mathrm{sgn}_{t\in(t_i,t_{i+1})}(\frac{\mathrm{d}B(x(t))}{\mathrm{d}t})$. With the conditions (5) and (6), t_n is the only local maximum of $B(x(t))$ $(t\in(t_0,+\infty))$. With $B(x(t))\in C^2(\chi)$ and condition (5), we can confirm $\frac{\mathrm{d}B(x(t))}{\mathrm{d}t}>0$ $(t\in(t_0,t_n))$. Thus, t_n is the maximum of $B(x(t))$ $(t\in(t_0,+\infty))$. With the condition (5), $B(x(t))<0$ $(t\in[t_0,+\infty))$.

(iii) Among $t_1,t_2,\ldots,t_{n-1}$, there are some extreme points. We can mark them as t_{ζ_j} $(j=1,2,\ldots,k)$ and k has $k\leqslant n-1$. It also has $t_1\leqslant t_{\zeta_1}\leqslant t_{\zeta_2}\leqslant\cdots\leqslant t_{\zeta_k}\leqslant t_{n-1}$. As t_n is the local maximum point, we can show that t_{ζ_k} is a local minimum point.

(a) If k is even, with Lemma 1, it can be shown that t_{ζ_1} is a local maximum. With $B(x(t))\in C^2(\chi)$ and condition (5), we can show $\frac{\mathrm{d}B(x(t))}{\mathrm{d}t}>0$ $(t\in(t_0,t_{\zeta_1}))$. Therefore, t_{ζ_1} is the maximum of $B(x(t))$ $(t\in[t_0,t_{\zeta_1}])$. With condition (5), $B(x(t))<0$ $(t\in[t_0,t_{\zeta_1}])$.

(b) If k is odd, then with the Lemma 1, it can be shown that t_{ζ_1} is a local minimum. With $B(x(t))\in C^2(\chi)$ and condition (5), we can show $\frac{\mathrm{d}B(x(t))}{\mathrm{d}t}<0$ $(t\in(t_0,t_{\zeta_1}))$. Thus, t_{ζ_1} is the minimum of $B(x(t))$ $(t\in[t_0,t_{\zeta_1}])$. Moreover, with condition (5), the condition $B(x(t))<0$ $(t\in[t_0,t_{\zeta_1}])$ holds.

(c) With (i) and (ii) in this proof, there always exists $B(x(t))<0$ $(t\in[t_0,t_{\zeta_1}])$. Also, for $[t_{\zeta_1},t_{\zeta_k}]\cup[t_{\zeta_k},t_n]=[t_{\zeta_1},t_n]$, by applying Lemma 3 and condition (5), we can show that it has $B(x(t))<0$ $(t\in[t_{\zeta_1},t_n])$. With conditions (5) and (6), we can obtain $B(x(t))<B(x(t_n))<0$ $(t\in(t_n,+\infty))$.

In summary, if there exists a barrier function $B(x)$ $(B(x)\in C^2(\chi))$, which satisfies conditions (3)–(6) for the system (1) where $f(x)$ is $C^2(\chi,\mathbb{R}^m)$ and the initial state x_0 has $x_0=x(t_0)\in\chi_0$, implying that the system is safe.

Corollary 1 (sufficient condition)**.** At some time t_0^*, when system (1), which is safe, turns to be system (2) with $f(x)\in C^2(\chi,\mathbb{R}^m)$ and $f_d(t)\in C^2(\mathbb{R},\mathbb{R}^m)$, system (2) can be referred to as a fault safety system from the moment t_0^* if there exists a function $\phi(x)$ $(\phi(x)\in C^2(\chi))$ satisfying

$$\begin{aligned}&\phi(x)<0\ (\forall x\in\chi_0), \qquad (7)\\&\phi(x)>0\ (\forall x\in\chi_u), \qquad (8)\\&\frac{\partial\phi}{\partial x}(x(t_i))[f(x(t_i))+f_d(t_i)]=0, \quad i=1,2,\ldots,n,\\&\phi(x(t_i))<0, \quad i=1,2,\ldots,n, \qquad (9)\\&\frac{\mathrm{d}^2\phi(x(t_n))}{\mathrm{d}t^2}<0,\\&\frac{\partial\phi}{\partial x}(x(t))[f(x(t))+f_d(t)]<0\ (t>t_n), \qquad (10)\end{aligned}$$

where $\frac{\partial\phi}{\partial x}(x(t))[f(x(t))+f_d(t)]=\frac{\mathrm{d}\phi(x(t))}{\mathrm{d}t}$, and n denotes a finite positive integer for condition (9).

Proof. The same proving process and principles as Theorem 1.

3.2 Analysis and discussion

For Theorem 1, if we want to rewrite the condition (11), where we remove the condition $\frac{\mathrm{d}^2B(x(t))}{\mathrm{d}t^2}<0$, and assume t_i $(1\leqslant i\leqslant n)$ is not the extreme point of the $B(x(t))$, then we can show that $\frac{\partial B}{\partial x}(x(t))f(x(t))\leqslant 0$

and $B(x(t)) \leqslant 0$ ($t \in [t_0, +\infty)$), which are very close to the key sufficient condition of Prajna et al. [21] and Romdlony et al. [20].

In addition, we do not need t_n to be the solution to $\dot{B} = 0$ and the last extreme point of function B at the same time. Therefore, we can update Theorem 1 to Theorem 2.

Theorem 2 (sufficient condition)**.** The system described by Eq. (1) where $f(x)$ is $C^2(\chi, \mathbb{R}^m)$ and the initial state x_0 has $x_0 = x(t_0) \in \chi_0$ can be said to be safe if there is a barrier function $B(x)$ ($B(x) \in C^2(\chi)$) satisfying

$$B(x) < 0 \ (\forall x \in \chi_0), \tag{11}$$

$$B(x) > 0 \ (\forall x \in \chi_u), \tag{12}$$

$$\begin{aligned} &\frac{\partial B}{\partial x}(x(t_i))f(x(t_i)) = 0, \quad i = 1, 2, \ldots, n, \\ &B(x(t_i)) < 0, \quad i = 1, 2, \ldots, n, \\ &\frac{\mathrm{d}^2 B(x(t_\eta))}{\mathrm{d}t^2} < 0 \ (t_1 \leqslant t_\eta \leqslant t_n), \end{aligned} \tag{13}$$

$$\frac{\partial B}{\partial x}(x(t))f(x(t)) < 0 \ (t > t_n), \tag{14}$$

where n denotes a finite positive integer and t_η is the last extreme point of $B(x(t))$ for condition (13).

Proof. With the proof of the Theorem 1, we can easily get $B(x(t)) < 0$ ($t \in [t_0, t_\eta]$). As t_η is the last extreme point of $B(x(t))$, condition (14) and $B(x) \in C^2(\chi)$, we can get:

(i) if $t_\eta = t_n$, it seems that the Theorem 2 is consistent with the description of Theorem 1. Therefore, it is true.

(ii) if $t_\eta < t_n$, $t_{\eta+1}, \ldots, t_n$ are not extreme points. According to the proof (ii) for Theorem 1, set $j = \eta + 1, \ldots, n$, and we can get $\mathrm{sgn}_{t\in(t_{j-1},t_j)}(\frac{\mathrm{d}B(x(t))}{\mathrm{d}t}) = \mathrm{sgn}_{t\in(t_n,+\infty)}(\frac{\mathrm{d}B(x(t))}{\mathrm{d}t})$. Then, we can show that $0 > B(x(t_\eta)) > B(x(t))$ ($t \in (t_\eta, +\infty)$). Thus, it has $B(x(t)) < 0$ ($t \in (t_0, +\infty)$).

With (i) and (ii) in this proof, therefore, Theorem 2 is established.

Corollary 2 (sufficient condition)**.** At some time t_0^*, when system (1), which is safe, turns to be system (2) with $f(x) \in C^2(\chi, \mathbb{R}^m)$ and $f_d(t) \in C^2(\mathbb{R}, \mathbb{R}^m)$, the system (2) can be called a fault safety system from the moment t_0^* if there exists a function $\phi(x)$ ($\phi(x) \in C^2(\chi)$) satisfying

$$\phi(x) < 0 \ (\forall x \in \chi_0), \tag{15}$$

$$\phi(x) > 0 \ (\forall x \in \chi_u), \tag{16}$$

$$\begin{aligned} &\frac{\partial \phi}{\partial x}(x(t_i))[f(x(t_i)) + f_d(t_i)] = 0, \quad i = 1, 2, \ldots, n, \\ &\phi(x(t_i)) < 0, \quad i = 1, 2, \ldots, n, \\ &\frac{\mathrm{d}^2 \phi(x(t_\eta))}{\mathrm{d}t^2} < 0 \ (t_1 \leqslant t_\eta \leqslant t_n), \end{aligned} \tag{17}$$

$$\frac{\partial \phi}{\partial x}(x(t))[f(x(t)) + f_d(t)] < 0 \ (t > t_n), \tag{18}$$

where n denotes a finite positive integer and t_η is the last extreme point of $\phi(x(t))$ for condition (19).

Proof. It can be easily proved by using Theorem 2.

3.3 Improvement of previous work

The constraints applied in this article and previous work [26] can be regarded as a type of extreme points. This article is for the case of finite extreme points while the previous work is for the case of infinite extreme points. With the deepening of our present research work, we find that the infinite extreme-point constraint proposed in the previous work still has some improvement space for constraint weakening. Therefore, there are sufficient safety criteria proposed in the following Theorem 3, where the important improvement is that Theorem 3 has removed the condition $\frac{\mathrm{d}^2 B(x(t_i))}{\mathrm{d}t^2} \neq 0$ from the original theorem.

Theorem 3 (sufficient condition)**.** The system (1) where $f(x)$ is $C^2(\chi, \mathbb{R}^m)$ and the initial state x_0 has $x_0 = x(t_0) \in \chi_0$ can be said to be safe if there is a barrier function $B(x)$ $(B(x) \in C^2(\chi))$ satisfying

$$B(x) < 0\ (\forall x \in \chi_0), \tag{19}$$

$$B(x) > 0\ (\forall x \in \chi_u), \tag{20}$$

$$\begin{aligned} &\frac{\partial B}{\partial x}(x(t_i))f(x(t_i)) = 0,\\ &B(x(t_i)) < 0,\\ &i = 1, 2, \ldots, n\ (n \to +\infty). \end{aligned} \tag{21}$$

Proof. (i) if $\frac{\partial B}{\partial x}(x(t))f(x(t)) \equiv 0$, we can show that $B(x(t)) < 0$ $(t \geqslant t_0)$ by applying condition (21).

(ii) According to the proof (ii) for Theorem 1, we know that if $t = t_i$ is not an extreme point of $B(x(t))$, then the same values of $\mathrm{sgn}(\frac{\mathrm{d}B(x(t))}{\mathrm{d}t})$ exist in the neighborhood of $t = t_i$ with the condition (21). Applying $B(x(t)) \in C^2(\chi)$ and condition (21), $t = t_i$, which is not the extreme point, does not change the monotonicity of the equation.

(a) There is only one extreme point. If this point is the local maximum point, any left side of this point is monotonically increasing, and any right side is monotonically reduced. Thus, by the condition (21), $B(x(t)) < 0$ $(t \geqslant t_0)$ is true.

If the point is the local minimum, any right side of this point is monotonically increasing, and any left side is monotonically reduced. Further, there will be no point such that $B(x(t)) > 0$. By applying condition (21) and $B(x(t)) \in C^2(\chi)$, if there exists a point making $B(x(t)) > 0$, there must be another extreme point, and the point must be the local maximum point. This contradicts the assumption that there is only one extreme point that is the local minimum.

(b) There are at least two extreme points. By applying Lemmas 1–3, we can make sure that $B(x(t)) < 0$ is true between any adjacent two extreme points. Furthermore, by applying assumption (a) in this proof (ii), there is $B(x(t)) < 0$ in the left side of the first extreme point and in the right side of the last extreme point t_e^*, where any $t_i > t_e^*$ only satisfies $\frac{\partial B}{\partial x}(x(t))f(x(t)) = 0$ but is not an extreme point.

(c) There are infinite extreme points. By applying Theorem 2 in [26], we can show that $B(x(t)) < 0$ $(t \geqslant t_0)$ is true.

Therefore, Theorem 3 is established.

Corollary 3 (sufficient condition)**.** At some time t_0^*, when system (1), which is safe, turns to be the system (2) with $f(x) \in C^2(\chi, \mathbb{R}^m)$ and $f_d(t) \in C^2(\mathbb{R}, \mathbb{R}^m)$, system (2) can be said to be fault safety from the moment t_0^* if there exists a function $\phi(x)$ $(\phi(x) \in C^2(\chi))$ satisfying

$$\phi(x) < 0\ (\forall x \in \chi_0), \tag{22}$$

$$\phi(x) > 0\ (\forall x \in \chi_u), \tag{23}$$

$$\begin{aligned} &\frac{\partial \phi}{\partial x}(x(t_i))[f(x(t_i))+f_d(t_i)] = 0,\\ &\phi(x(t_i)) < 0,\\ &i = 1, 2, \ldots, n\ (n \to +\infty). \end{aligned} \tag{24}$$

Proof. We can prove it by using Theorem 3.

4 Constructive design of barrier function

In our previous work, we proposed a simple construction method for the barrier function under a single closed unsafe set [26]. Assume that there is a real unsafe set $\widetilde{\chi}_u$, which is simply-connected and bounded. Set the centroid of the set to x_o and the maximum distance from the centroid to the boundary $\partial\widetilde{\chi}_u$ as r. Further, we construct a hypersphere χ_u $(\widetilde{\chi}_u \subseteq \chi_u)$ with a center point x_o and radius r, where the hypersphere is a circle when $\dim x_0$ is 2 and a ball when $\dim x_0$ is 3. Therefore, the corresponding barrier function $B(x) = r - \|x - x_o\|_2$ satisfies $B(x) \leqslant 0, \forall x \in \chi_0$ and $B(x) > 0, \forall x \in \chi_u$. The same is applicable to $\phi(x)$.

This approach is highly conservative for a single closed unsafe set with complex geometry that divides a portion of the safety state into the formed hypersphere. Therefore, we need to find an optimization method based on this method that makes $\chi_u \cap (\chi \backslash \widetilde{\chi}_u) = 0$ true. To make the calculation more convenient, we need to rebuild the barrier function, which is now

$$B(x) = r^2 - \|x - x_o\|_2^2. \tag{25}$$

Such a method can be termed the hypersphere construction method of barrier function, which can be shortened to the hypersphere method.

However, sometimes by using only one hypersphere by (25), we may not be able to obtain an expected result. According to Corollary 4.1 proposed by Kong et al. [23], it is feasible to construct multiple BFs satisfying the conditions (11)–(13) [23] in a unified form to represent or cover all of the unsafe set or sets. We can learn from the ideas presented in [23] to design a set of hyperspheres to cover multiple unsafe sets. Moreover, if the unsafe set of system (1) is single and closed with complex geometry or is complex connected, we can also wrap or cover unsafe sets by using multiple combinations of hyperspheres. These two situations can be handled in a similar manner. Thus, we refer to this method as the multi-hypersphere method.

Theorem 4. If $u = \varphi(x)$ is derivable at the point x_0, and $y = h(u)$ is derivable at the point $u_0 = \varphi(x_0)$, then the composite function $h \circ \varphi$ is derivable at the point x_0.

Proof. The details can be found in page 99 of [40].

Theorem 5 (sufficient condition)**.** Suppose the unsafe set χ_u is bounded and simple-connected. There exist a set of hyperspheres $\Omega_1(x_{o_1}, r_1), \ldots, \Omega_K(x_{oK}, r_K)$ where each center of these has $x_{o_i} \in \chi_u$ $(1 \leqslant i \leqslant K)$ and $B_i(x) = r_i^2 - \|x - x_{o_i}\|_2^2$. If these hyperspheres satisfy $\chi_u \subseteq \bigcup_{i=1}^K \Omega_i$ and the following conditions:

$$\forall x \in \chi_0 : \bigwedge_{i=1}^{K} B_i(x) < 0, \tag{26}$$

$$\forall x \in \chi : \bigwedge_{i=1}^{K} \begin{array}{l} \dfrac{\partial B_i}{\partial x}(x(t_j)) f(x(t_j)) = 0, \quad j = 1, \ldots, n, \\ B_i(x(t_j)) < 0, \quad j = 1, \ldots, n, \\ \dfrac{\mathrm{d}^2 B_i(x(t_n))}{\mathrm{d}t^2} < 0, \\ \dfrac{\partial B_i}{\partial x}(x(t)) f(x(t)) < 0 \ (t > t_n), \end{array} \tag{27}$$

$$\forall x \in \chi_u : \bigvee_{i=1}^{K} B_i(x) > 0, \tag{28}$$

where $\frac{\partial B_i}{\partial x}(x(t)) f(x(t)) = \frac{\mathrm{d}B_i(x(t))}{\mathrm{d}t}$and n denotes a finite positive integer for condition (24) where there is no t_ζ, which has $\frac{\partial B_i}{\partial x}(x(t_\zeta)) f(x(t_\zeta)) = 0$. Then the system (1) ,where $f(x)$ is $C^2(\chi, \mathbb{R}^m)$, can be said to be safe.

Proof. At first, we have to prove that the BFs $B_i(x)$ $(1 \leqslant i \leqslant K)$ satisfying $B_i(x(t))$ is second-order continuously differentiable in $t \geqslant t_0$.

As already established, $B_i(x) = r_i^2 - \|x - x_{o_i}\|_2^2$. By simultaneously deriving the time t on the both sides, we can show that

$$\frac{\mathrm{d}B_i(x)}{\mathrm{d}t} == -2(x - x_{o_i})^{\mathrm{T}} f(x). \tag{29}$$

By applying Theorem 4, we can show that $\frac{\mathrm{d}B_i(x)}{\mathrm{d}t}$ is derivable in $t \geqslant t_0$. According to theorem [35], if the function is derivable at a certain point, that is, the function is continuous at that point, we can show that $B_i(x(t))$ is continuous in $t \geqslant t_0$, by (29). With Eq. (29) and simultaneously deriving the time t on the both sides, we have

$$\frac{\mathrm{d}^2 B_i(x)}{\mathrm{d}t^2} = -2f^{\mathrm{T}}(x) f(x) - 2(x - x_{o_i})^{\mathrm{T}} \frac{\partial f(x)}{\partial x} f(x). \tag{30}$$

So, we can show that $B_i(x(t))$ is first-order continuously differentiable in $t \geqslant t_0$. With the same process, we can finally show that $B_i(x(t))$ is second-order continuously differentiable in $t \geqslant t_0$.

By applying Corollary 4.1 [23] and Theorem 2, and having proved that $B_i(x(t))$ is second-order continuously differentiable in $t \geqslant t_0$, we can say that Theorem 5 is established.

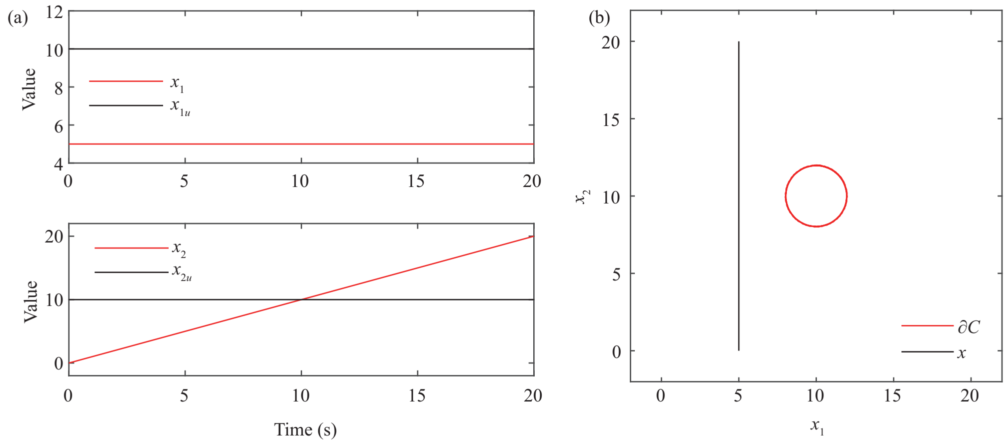

Figure 1 (Color online) State x of Example 1. (a) Dynamic time-varying; (b) the relation between x and unsafe set χ_u.

However, how do we choose the barrier function to use? The question in this section seemingly refers to when we should use only one hypersphere and when we should use multiple hyperspheres. When we need to build a barrier function for a single unsafe set, first, we can try to design a single hypersphere by using Eq. (25). If the sacrifice of feasible states close to the original unsafe state set can be acceptable, we can continue to use the designed single hypersphere. If the sacrifice is great, we have to use a set of available hyperspheres similar to Theorem 5. Therefore, we have to establish a sacrifice assessment function and sacrifice acceptance threshold. To the former, we can calculate the mass of the sacrificed parts where these parts have geometrical "area", "volume", with different values of $\dim x$, assuming that the density is $\rho = 1$. To the latter, it may be a threshold set by experience.

Moreover, for multiple unsafe sets, we need to use a series of hyperspheres and utilize the above method to handle every unsafe set.

5 Examples

Example 1. Consider a dynamic system defined as

$$\dot{x}(t) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad x(t_0) = x_0, \tag{31}$$

with an unsafe set $\chi_u = \{x \in \mathbb{R}^2 : \|x - x_u\|_2 \leqslant r\}$. Herein, we use a barrier function $B(x) = r^2 - \|x - x_u\|_2^2$, such that it satisfies

$$\begin{cases} B(x) > 0, & \forall x \in \chi_u, \\ B(x) \leqslant 0, & \forall x \in \chi_s, \end{cases} \tag{32}$$

where $\chi_s =: \mathbb{R}^2 \backslash \chi_u$. Suppose that $x_0 = (\frac{x_{1u}}{2}, 0)^{\mathrm{T}}$ and $r \in (0, \frac{x_{1u}}{2})$. Then, we can have

$$\dot{B} = -2(x_2(t) - x_{2u}), \tag{33}$$

$$\ddot{B} = -2\dot{x}_2 = -2. \tag{34}$$

Hence, when $x_2(t_*) = x_{2u}$, $B(x(t_*))$ is the only local max extreme value and is the maximum. At this time, it has

$$B(x(t_*)) = r^2 - \frac{x_{1u}^2}{4} < 0.$$

Therefore, by applying Theorem 1, we can show that the system described by Eq. (31) is safe, as shown in Figures 1 and 2, with $r = 2$ and $x_u = (10, 10)^{\mathrm{T}}$. The initial state $x_0 = (\frac{x_{1u}}{2}, 0)^{\mathrm{T}} = (5, 0)^{\mathrm{T}}$. We set the initial time to zero.

The state $x(t)$ from the initial point $(5, 0)$ moves straight to the final point $(5, 20)$ in Figure 1(b). Therefore, from Figure 1, we can find the system state x will never enter the unsafe set because it has initial state x_0, where the trajectory of state x is parallel to the unsafe set in space. However, if we

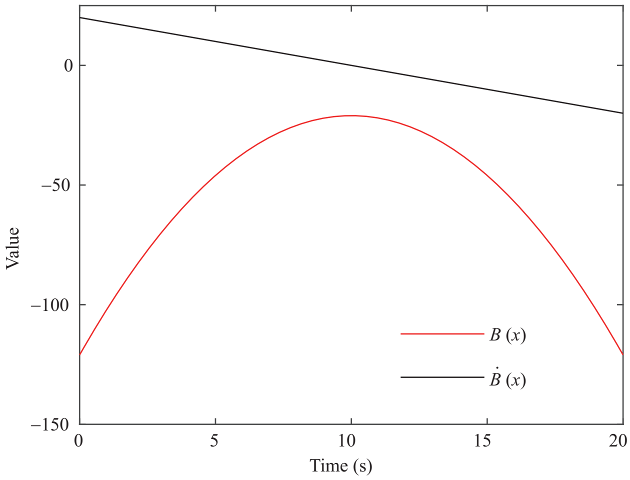

Figure 2 (Color online) Dynamic changes of B and $\dot{B}$ of Example 1.

only see Figure 1(a), with the intersection of the line x_2 and the line x_{2u}, we may have the illusion that x enters into the unsafe set at the point where the time is 10 s. Variation in the value of $B(x(t))$ is experienced by first increasing and then decreasing the value with a maximum at time 10 s and keeping it negative throughout the simulation time, which also implies that the relative distance between $x(t)$ and the unsafe set χ_u follows the process from far to near, from near to far, as shown in Figure 2. Therefore, Figures 1 and 2 show the safety of the system (31).

Example 2. Consider a dynamic system defined as

$$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \end{pmatrix} = \begin{pmatrix} -x_2 + x_{2u} \\ x_1 - \dfrac{x_{1u}}{2} \end{pmatrix}, \quad x(t_0) = x_0, \tag{35}$$

where $x = \binom{x_1}{x_2}$, $r < \frac{x_{1u}}{4}$. It has an unsafe set χ_u and other state set $\chi_s = \mathbb{R}^2 \backslash \chi_u$, and $\chi_u = \{x \in \mathbb{R}^2 : \|x - x_u\|_2 \leqslant r\}$.

Thus, we can have

$$\begin{cases} x_1 = \dfrac{x_{1u}}{2} + r\cos t, \\ x_2 = x_{2u} + r\sin t, \end{cases} \quad \begin{cases} \dot{x}_1 = -r\sin t, \\ \dot{x}_2 = r\cos t. \end{cases} \tag{36}$$

We can choose a barrier function $B(x) = r^2 - \|x - x_u\|_2^2$. Thus, we can have

$$\dot{B} = -2(x - x_u)^{\mathrm{T}} \begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \end{pmatrix} = -x_{1u} r \sin t. \tag{37}$$

When Eq. (37) becomes zero, we can have $t = n\pi$ $(n \to \infty)$. This implies that

$$B(x(t)) = \begin{cases} x_{1u} r - \dfrac{x_{1u}^2}{4} < 0, & t = 2k\pi, \\ -x_{1u} r - \dfrac{x_{1u}^2}{4} < 0, & t = (2k+1)\pi. \end{cases} \tag{38}$$

Therefore, by Theorem 3, we can show that the system described by (35) is safe, as shown in Figures 3 and 4, with $r = 2$ and $x_u = (10, 10)^{\mathrm{T}}$. The initial state is $(5, 10)$ and $t_0 = 0$. From Figure 3(a), we find $x_1(t)$ fluctuating cosine and $x_2(t)$ fluctuating sine, which are consistent with the derived formula (36). Thus, the state $x(t)$ seems to imply that the system is performing a circular motion as shown by Figure 3(b), and we can find a trajectory of state x parallel to the unsafe set χ_u in space. It makes the value of $B(x(t))$ and its derivative fluctuate periodically, and there are both maximum and minimum values of $B(x(t))$ within each period. Hence, the relative distance between x and χ_u also follows the process from near to far, from far to near, and iterates continuously as shown in Figure 4.

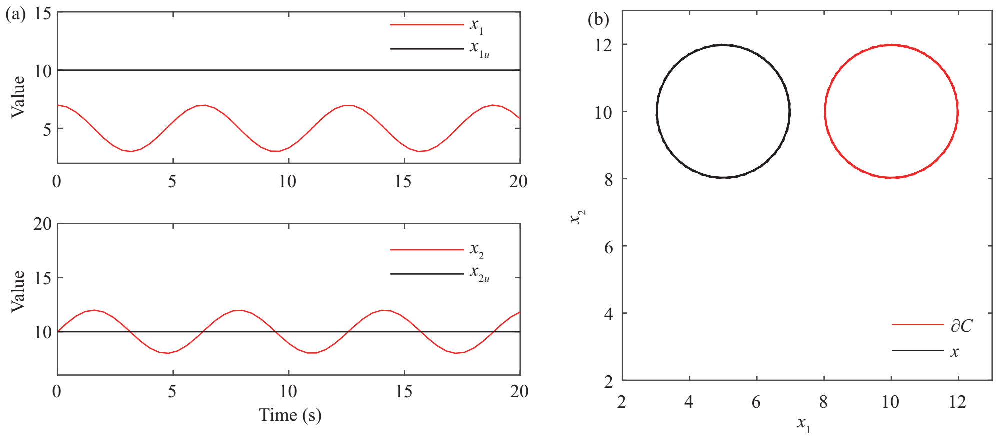

Figure 3 (Color online) State x of Example 2. (a) Dynamic time-varying; (b) the relation between x and unsafe set χ_u.

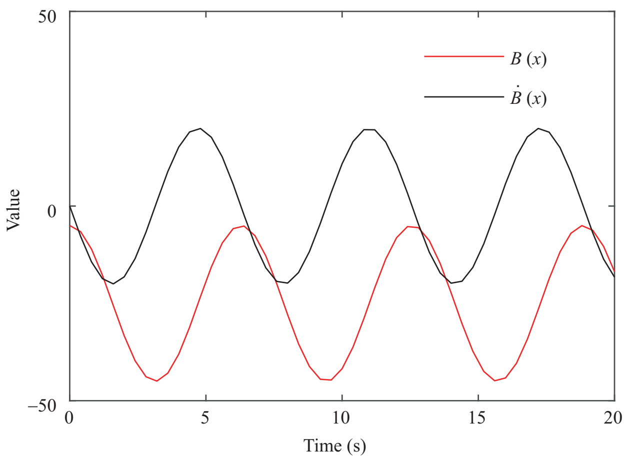

Figure 4 (Color online) Dynamic changes of B and $\dot{B}$ of Example 2.

Example 3. Consider a dynamic system defined as

$$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \end{pmatrix} = \begin{pmatrix} -x_2 + x_{2u} \\ x_1 - x_{1u} \end{pmatrix}, \quad x(t_0) = x_0, \tag{39}$$

where $x = \binom{x_1}{x_2}$, $r < \frac{x_{1u}}{4}$. The system has an unsafe set χ_u and other state set $\chi_s = \mathbb{R}^2 \backslash \chi_u$, where $\chi_u = \left\{x \in \mathbb{R}^2 : \|x - x_u\|_2 \leqslant r\right\}$. Hence, we can have

$$\begin{cases} x_1 = x_{1u} + 2r\cos t, \\ x_2 = x_{2u} + 2r\sin t, \end{cases} \quad \begin{cases} \dot{x}_1 = -2r\sin t, \\ \dot{x}_2 = 2r\cos t. \end{cases} \tag{40}$$

We choose a barrier function $B(x) = r^2 - \|x - x_u\|_2^2$. Then, we have

$$\dot{B} = -2(x - x_u)^{\mathrm{T}} \begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \end{pmatrix} = 0. \tag{41}$$

It implies that

$$B(x(t)) = -3r^2. \tag{42}$$

Therefore, by applying Theorem 3, we can show that the system (39) is safe as shown in Figures 5 and 6, with $r = 2$ and $x_u = (10, 10)^{\mathrm{T}}$. The initial state is $(14, 10)$ and $t_0 = 0$. From Figure 5(a), we can see that $x_1(t)$ is a fluctuating cosine and $x_2(t)$ is a fluctuating sine, which are consistent with (40). Hence, at state $x(t)$ the system actually performs a circular motion as shown in Figure 5(b), and we can see that

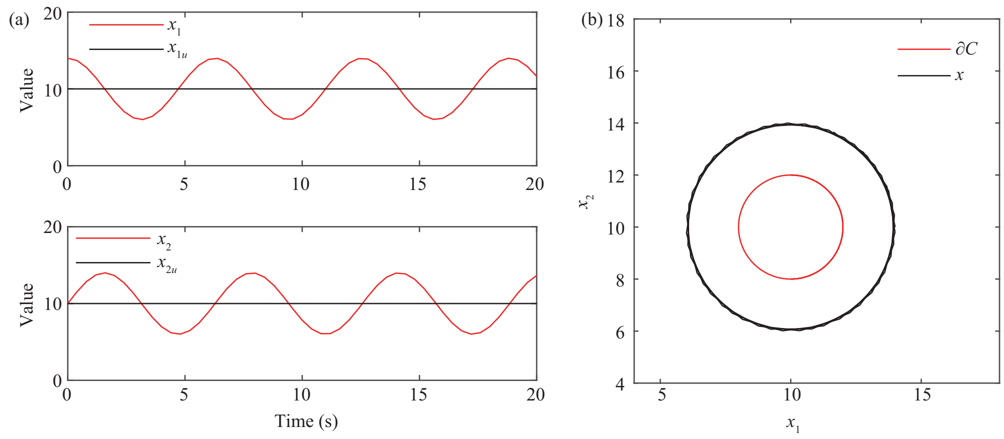

Figure 5 (Color online) State x of Example 3. (a) Dynamic time-varying; (b) the relation between x and unsafe set χ_u.

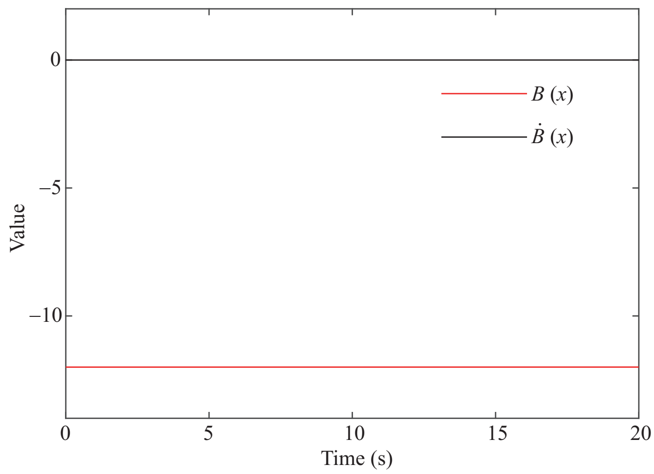

Figure 6 (Color online) Dynamic changes of B and $\dot{B}$ of Example 3.

this mode of motion of state x is akin to a synchronous orbiting satellite in orbit of the unsafe set χ_u. Thus, the value of the barrier function $B(x(t))$ is a negative constant and its derivative is 0, proved by Figure 6.

6 Conclusion

We have put forward and proved Theorems 1–3 and Corollaries 1–3. Theorems 1 and 2 can be regarded as an improved and extended theorem, where we relax the condition that the last point t_n making $\dot{B} = 0$ does not need to be an extreme point, while the last point t_n in Theorem 1 must be an extreme point, particularly a local maximum point. We demonstrated Theorem 3, which is more like a fusion form of Theorem 2 in our previous work [26] and Theorems 1 and 2 in this paper. Corollaries 1–3 are the deformation and derivative criteria of Theorems 1–3 when a fault occurs during the operation of the system. The fault introduced herein should be measurable or can be estimated.

According to our guess, the theorems or corollaries proposed in this paper may be more suitable for a class of dynamic systems with periodic, non-uniform periodic or with reciprocating characteristics or estimable faults with intermittent characteristics. However, we did not verify their applicability or universality. Such a verification is quite a challenge for which we have not found an adequate solution at the moment.

We believe that the sufficient conditions of the barrier functions, which were posited by Prajna, Kong, and our work, can be considered a fusion and can then be described with a set of unified mathematical expressions that cover all three different judgement conditions. This comprises our future work and the objective that we have been working hard to achieve.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61633005).

References

1 Chai Y, Zhang K, Mao Y F, et al. Technology of Dynamic System Operational Safety (in Chinese). Beijing: Chemical Industry Press, 2019
2 Chai Y, Mao W B, Ren H, et al. Research on operational safety assessment for spacecraft launch system: progress and challenges (in Chinese). Acta Autom Sin, 2019, 45: 1829–1845
3 Bouamama B O, Biswas G, Loureiro R, et al. Graphical methods for diagnosis of dynamic systems: review. Annu Rev Control, 2014, 38: 199–219
4 Kasai N, Fujimoto Y, Yamashita I, et al. The qualitative risk assessment of an electrolytic hydrogen generation system. Int J Hydrogen Energy, 2016, 41: 13308–13314
5 Cunha S B. A review of quantitative risk assessment of onshore pipelines. J Loss Prevent Process Ind, 2016, 44: 282–298
6 Ahn J, Chang D. Fuzzy-based HAZOP study for process industry. J Hazard Mater, 2016, 317: 303–311
7 Chang Y Q, Han Z F, Zou X T. Online assessment of complex industrial processes operating performance based on improved dynamic causality diagram (in Chinese). Control Theory Appl, 2017, 34: 345–354
8 Khan F, Hashemi S J, Paltrinieri N, et al. Dynamic risk management: a contemporary approach to process safety management. Curr Opin Chem Eng, 2016, 14: 9–17
9 Naderpour M, Lu J, Zhang G Q. An abnormal situation modeling method to assist operators in safety-critical systems. Reliab Eng Syst Saf, 2015, 133: 33–47
10 Villa V, Paltrinieri N, Khan F, et al. Towards dynamic risk analysis: a review of the risk assessment approach and its limitations in the chemical process industry. Saf Sci, 2016, 89: 77–93
11 Busby J S, Green B, Hutchison D. Analysis of affordance, time, and adaptation in the assessment of industrial control system cybersecurity risk. Risk Anal, 2017, 37: 1298–1314
12 Li H T. Research on safety analysis method based on safety risk state (in Chinese). Dissertation for Ph.D. Degree. Changsha: National University of Defense Technology, 2012
13 Kriaa S, Pietre-Cambacedes L, Bouissou M, et al. A survey of approaches combining safety and security for industrial control systems. Reliab Eng Syst Saf, 2015, 139: 156–178
14 Talebberrouane M, Khan F, Lounis Z. Availability analysis of safety critical systems using advanced fault tree and stochastic Petri net formalisms. J Loss Prevent Process Ind, 2016, 44: 193–203
15 Guo Y B, Meng X L, Wang D G, et al. Comprehensive risk evaluation of long-distance oil and gas transportation pipelines using a fuzzy Petri net model. J Nat Gas Sci Eng, 2016, 33: 18–29
16 Wang X, Mahulea C, Silva M. Diagnosis of time Petri nets using fault diagnosis graph. IEEE Trans Autom Control, 2015, 60: 2321–2335
17 Landucci G, Argenti F, Cozzani V, et al. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf Environ Protection, 2017, 110: 102–114
18 Barua S, Gao X D, Pasman H, et al. Bayesian network based dynamic operational risk assessment. J Loss Prevention Process Ind, 2016, 41: 399–410
19 Ye L B. A study on operation safety analysis and online assessment of industrial processes (in Chinese). Dissertation for Ph.D. Degree. Hangzhou: Zhejiang University, 2011
20 Romdlony M Z, Jayawardhana B. Stabilization with guaranteed safety using control Lyapunov-barrier function. Automatica, 2016, 66: 39–47
21 Prajna S, Rantzer A. On the necessity of barrier certificates. In: Proceedings of the 16th IFAC World Congress, Prague, 2005. 526–531
22 Prajna S, Jadbabaie A, Pappas G J. Stochastic safety verification using barrier certificates. In: Proceedings of IEEE Conference on Decision and Control, 2004
23 Kong H, Song X Y, Han D, et al. A new barrier certificate for safety verification of hybrid systems. Comput J, 2014, 57: 1033–1045
24 Wang G B, He J F, Liu J, et al. Safety verification of interconnected hybrid systems using barrier certificates. Math Problem Eng, 2016, 2016: 1–10
25 Wang G B, Liu J, Sun H Y, et al. Safety verification of state/time-driven hybrid systems using barrier certificates. In: Proceedings of the 35th Chinese Control Conference (CCC), 2016. 2483–2489
26 Zhu Z R, Chai Y, Yang Z M. A novel kind of sufficient conditions for safety judgement based on control barrier function. Sci China Inf Sci, 2021, 64: 199205
27 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 Annual Conference on Decision and Control (CDC), 2014. 6271–6278
28 Xu X R, Tabuada P, Grizzle J W, et al. Robustness of control barrier functions for safety critical control. IFAC-PapersOnLine, 2015, 48: 54–61

29 Glotfelter P, Cortes J, Egerstedt M. Nonsmooth barrier functions with applications to multi-robot systems. IEEE Control Syst Lett, 2017, 1: 310–315

30 Borrmann U, Wang L, Ames A D, et al. Control barrier certificates for safe swarm behavior. IFAC-PapersOnLine, 2015, 48: 68–73

31 Wang L, Ames A D, Egerstedt M. Safety barrier certificates for collisions-free multirobot systems. IEEE Trans Robot, 2017, 33: 661–674

32 Wang L, Ames A, Egerstedt M. Safety barrier certificates for heterogeneous multi-robot systems. In: Proceedings of American Control Conference (ACC), Boston, 2016. 5213–5218

33 Ames A D, Xu X, Grizzle J W, et al. Control barrier function based quadratic programs for safety critical systems. IEEE Trans Autom Control, 2017, 62: 3861–3876

34 Agrawal A, Sreenath K. Discrete control barrier functions for safety critical control of discrete systems with application to bipedal robot navigation. In: Proceedings of Robotics: Science and Systems Conference, Cambridge, 2017

35 Tong S C, Li Y M. Observer-based adaptive fuzzy backstepping control of uncertain nonlinear pure-feedback systems. Sci China Inf Sci, 2014, 57: 012204

36 Jain A K, Bhasin S. Tracking control of uncertain nonlinear systems with unknown constant input delay. IEEE/CAA J Autom Sin, 2020, 7: 420–425

37 Tong S C, Li Y M. Robust adaptive fuzzy backstepping output feedback tracking control for nonlinear system with dynamic uncertainties. Sci China Inf Sci, 2010, 53: 307–324

38 Gomes J P P, Galvao R K H, Yoneyama T, et al. A new degradation indicator based on a statistical anomaly approach. IEEE Trans Rel, 2016, 65: 326–335

39 Zheng J F, Si X S, Hu C H, et al. A nonlinear prognostic model for degrading systems with three-source variability. IEEE Trans Rel, 2016, 65: 736–750

40 Department of Mathematics, East China Normal University. Mathematical Analysis (in Chinese). 3rd. Beijing: Higher Education Press, 1999