SCIENCE CHINA
Information Sciences

• LETTER •

September 2021, Vol. 64 199205:1–199205:3
https://doi.org/10.1007/s11432-018-9840-6

A novel kind of sufficient conditions for safety judgement based on control barrier function

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

[1] *Key Laboratory of Complex System Safety and Control (Chongqing University), Ministry of Education, Chongqing 400044, China;*
[2] *School of Automation, Chongqing University, Chongqing 400044, China*

Received 14 December 2018/Revised 10 February 2019/Accepted 25 March 2019/Published online 29 June 2020

Citation 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(9): 199205, https://doi.org/10.1007/s11432-018-9840-6

Dear editor,

Recently, work safety accidents have started to occur on a large scale in Chinese petrochemical companies. Further, the operational safety of large and complex systems is being closely monitored by our government, environmental organizations, and conscientious citizens. The scale of complex systems, such as industrial systems and smart grids, has expanded because of the usage of new technologies, including cyber-physical systems and multi-agent systems. Additionally, it has become difficult to detect, control, and protect the operational safety. Because the information mapped by the physical world is becoming increasingly comprehensive, it has become imperative to effectively maintain operational safety in a specific kind of system. This area is receiving considerable attention in both the academic and the engineering fields. Therefore, operational safety will remain as fundamental as the operational stability required in a complex system.

Certain types of system operational analyses and control methods are considerably different; they are based on the control barrier function (CBF) [1] inspired by the Lyapunov stability analysis theory, which transforms the safety analysis problems into a class of analysis and calculation of the existence of solutions for reachability problems. For example, Prajna et al. [2,3], Kong et al. [4], and Wang et al. [5,6] proposed theorems for performing the safety analysis of hybrid systems or complex systems.

In this study, we use the research results of [2–6] and introduce an important system change with respect to the system operational fault. Further, we propose a mathematical description of the vital concepts related to fault safety with respect to the operational safety of the complex systems based on the system dynamics equations and CBF. Subsequently, we propose a novel sufficient condition for obtaining the CBF-based safety criterion.

Model and methodology. Based on [2], we consider the following kind of system:

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

where $f \in R^m$ represents the r-times continuously differentiable function $(1 < r \leqslant m)$ denoted by $C^r(\chi, R^m)$. The system state is denoted by $x(t) \in \chi \subseteq R^m$, the open unsafe set is denoted by $\chi_u \subseteq \chi$, and the initial state set is denoted by $\chi_0 \cap \chi_u = \emptyset$ $(\chi_0 \subseteq \chi)$. The system (1) can be considered to be safe if there does not exist a motion $\phi(t; x_0, t_0)$ of the system (1) with $x_0 = x(0) \in \chi_0$ and $\phi(t; x_0, t_0) = x(t)$, which makes the set $\Omega = \{\phi(t; x_0, t_0), t \in [0, T]\}$ have $\Omega \cap \chi_u \neq \emptyset$ for $T \to +\infty$.

Definition 1 (Fault safety)**.** At some time t_0^*, the system (1) contains a fault $f_d(t)$ with $f_d \in C^r(R, R^m)$ so that it transforms into the system (2) as follows:

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

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

Remark 1. The time constant T is only a finite value [2]. Now, T can approach infinity [1].

Theorem 1 (Sufficient condition)**.** At some time t_0^*, when the system (1) is turning into system (2), the system (2) can be referred to as a fault-safe system from the moment t_0^* to the moment T (the value of T is sufficiently large) if there exists a function $\psi(x) \in C^r(\chi, R)$ $(1 \leqslant r \leqslant m)$ satisfying

$$\psi(x) \leqslant 0, \quad \forall x \in \chi_0^*, \tag{3}$$

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

$$\frac{\partial \psi}{\partial x}(x(t))[f(x(t)) + f_d(t)] \leqslant 0, \ \forall x \in \chi/\chi_u. \tag{5}$$

Proof. As we know, $x(t_0^*) \in \chi_0^*$ and $x(t)$ denote the solutions of the system (2). If we can find one function $\psi(x(t)) \in C^r(\chi, R)$ that satisfies the conditions (3)–(5) and the following condition (6) [4], the system must be fault-safe.

$$\forall \theta \geqslant t_0^*, \quad \psi(x(\theta)) \leqslant 0. \tag{6}$$

[*] Corresponding author (email: luxucy1@qq.com)

Let $g(x) = \frac{\partial\psi}{\partial x}(x)[f(x) + f_d(t)]$. Further, with (5), we can obtain

$$\forall x \in \chi/\chi_u,\ g(x) \leqslant 0. \tag{7}$$

Because $\frac{\mathrm{d}\psi(x(t))}{\mathrm{d}t} = \frac{\partial\psi}{\partial x}\frac{\mathrm{d}x}{\mathrm{d}t} = \frac{\partial\psi}{\partial x}(x)[f(x) + f_d(t)]$, we obtain a first-order non-homogeneous ordinary differential equation about $\psi(x(t))$.

$$\frac{\mathrm{d}\psi(x(t))}{\mathrm{d}t} - g(x(t)) = 0\ (\psi(x(t_0^*)) = \psi(x_0^*)). \tag{8}$$

The following equation can be considered to be the solution of the differential equation (8).

$$\psi(x(t)) = \int_{t_0^*}^{t} g(x(\tau))\mathrm{d}\tau + \psi(x_0^*). \tag{9}$$

We can obtain the following from (3) and (7):

$$\psi(x(t)) = \int_{t_0^*}^{t} g(x(\tau))\mathrm{d}\tau + \psi(x_0^*) \leqslant 0. \tag{10}$$

Lemma 1. A function $h(x)$ $(x \in R, h(x) \in R)$ is r-times continuously differentiable $(r = 2)$. If $h(x)$ contains n $(n \geqslant 2)$ extreme points, any two adjacent extreme points must include a local maximum value and a local minimum value.

Proof. Assumption 1. Let a and b be any two adjacent extreme points of $h(x)$, which are the same as the local maximum or the local minimum of $h(x)$. Further, we can obtain $h'(a) = h'(b) = 0$ and $h''(a) \cdot h''(b) > 0$.

(1) Let us suppose that both a and b are the local maximums. $h''(a) < 0$, $h''(b) < 0$. Then there exist ϑ_1 and ϑ_2 such that $h'(x) < 0$ for $x \in (a, \vartheta_1)$, and $h'(x) > 0$ for $x \in (\vartheta_2, b)$.

By the root existence theorem [7], there is at least one $\vartheta_3 \in [\vartheta_1 - \delta, \vartheta_2 + \delta]$ $(\forall\delta > 0)$ satisfying $h'(\vartheta_3) = 0$.

Because $h(x)$ is twice continuously differentiable, we have $h'(x) \leqslant 0$ for $x \in (\vartheta_1, \vartheta_3)$, and $h'(x) \geqslant 0$ for $x \in (\vartheta_3, \vartheta_2)$.

We can obtain that $\vartheta_3 \in (a, b)$ is a local minimum. This does not correspond to the assumption that a and b are two adjacent extreme points. So Assumption 1 fails.

(2) Let us suppose that both a and b are local minimums. Then, we can prove in a similar manner that Assumption 1 is invalid.

Based on the above analysis, the proof is completed.

Lemma 2. A function $h(x) \in R$ is r-times continuously differentiable $(r = 2)$. If the maximum or minimum of $h(x)$ is $x_0 \in (a, b)$, x_0 must be the local maximum or the local minimum of $h(x)$.

Proof. (1) Let $x_0 \in (a, b)$ be the maximum of $h(x)$; then we can obtain $h(x_1) \leqslant h(x_0)$ for $x_1 \in (a, x_0)$, and $h(x_2) \leqslant h(x_0)$ for $x_2 \in (x_0, b)$.

Therefore, $\forall\delta > 0$, $x \in (x_0 - \delta, x_0)$, $h'(x) \geqslant 0$ and $x \in (x_0, x_0 + \delta)$, $h'(x) \leqslant 0$. So that x_0 is a local maximum of $h(x)$.

(2) Let $x_0 \in (a, b)$ be the minimum of $h(x)$. We can prove similarly that x_0 is a local minimum of $h(x)$.

With (1) and (2), the proof is completed.

Lemma 3. An r-times continuously differentiable function $h(x) \in R$ $(r = 2)$ has n $(n \geqslant 2)$ extreme points. Therefore, $h(\theta)$, $\theta \in (a, b)$, must satisfy $\min\{h(a), h(b)\} < h(\theta) < \max\{h(a), h(b)\}$, where a, b $(a < b)$ are any two adjacent extreme points.

Proof. (1) Assume that $h(\theta), \theta \in (a, b)$, is the maximum of $h(x)$. According to Lemma 2, θ is a local maximum of $h(x)$. This does not correspond to the assumption that a, b are two adjacent extreme points. So the assumption fails. We get $h(\theta) < \max\{h(a), h(b)\}$.

(2) Assume that $h(\theta), \theta \in (a, b)$, is the minimum of $h(x)$. In a similar manner, we can prove that the assumption is invalid. We get $h(\theta) > \min\{h(a), h(b)\}$. This completes the proof.

Theorem 2 (Sufficient condition)**.** The system (1), where $f(x)$ is $C^2(\chi, R^m)$, is safe if there exists a function $B(x)$ $(B(x) \in C^2(\chi))$ that satisfies

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

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

$$\begin{aligned}&\frac{\partial B}{\partial x}(x_i)f(x_i) = 0,\ \frac{\mathrm{d}^2B(x_i)}{\mathrm{d}t^2} \neq 0,\ B(x_i) \leqslant 0,\\ &\forall x_i \in \chi/\chi_u,\ x_i = x(t_i),\ 1 \leqslant i \leqslant n\ (n \to \infty).\end{aligned} \tag{13}$$

Proof. (1) If the initial state x_0 is located between any two adjacent extreme points, according to Lemmas 1–3 and the condition (13), we know $t \geqslant 0$, $B(x(t)) \leqslant 0$.

(2) If the initial state x_0 is located on the left side of the first local maximum point, according to Lemmas 2 and 3, $t \in [0, t_1]$, $B(x(t)) \leqslant B(x_1) \leqslant 0$. With Lemmas 1–3 and the condition (13), $t \geqslant t_1$, $B(x(t)) \leqslant 0$. So we get $t \geqslant 0$, $B(x(t)) \leqslant 0$.

(3) If x_0 is located on the left side of the first local minimum point, we can observe that $B(x(t))$ $(t \in [0, t_1])$ is a monotonic reduction function. Therefore, $t \in [0, t_1]$ and $B(x(t)) \leqslant B(x_0) < 0$. According to Lemmas 1–3 and the condition (13), we obtain $t \geqslant t_1, B(x(t)) \leqslant 0$. So we get $t \geqslant 0$, $B(x(t)) \leqslant 0$.

This completes the proof.

Corollary 1 (Sufficient condition)**.** At some time t_0^*, when the safe system (1) transforms into the system (2) with $f(x) \in C^2(\chi, R^m)$ and $f_d(t) \in C^r(R, R^m)$, the system (2) can be called a fault safe system from the moment t_0^* to the moment T (T is large enough) if there exists a function $\psi(x) \in C^2(\chi)$ satisfying

$$\psi(x) \leqslant 0,\quad \forall x \in \chi_0^*, \tag{14}$$

$$\psi(x) > 0,\quad \forall x \in \chi_u, \tag{15}$$

$$\begin{aligned}&\frac{\partial\psi}{\partial x}(x_i)[f(x_i)+f_d(t_i)]=0,\ \frac{\mathrm{d}^2\psi(x_i)}{\mathrm{d}t^2}\neq 0,\ \psi(x_i)\leqslant 0,\\ &\forall x_i\in\chi/\chi_u,\ x_i=x(t_i),\ 1\leqslant i\leqslant n\ (n\to\infty).\end{aligned} \tag{16}$$

Proof. The proof is the same as that of the Theorem 2.

Constructive design of a barrier function. We have to find an easy method for constructing a barrier function. Let us assume that there is a real unsafe set $\widetilde{\chi}_u$, which is a single open set. 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 the center point x_o and radius r, where the hypersphere is a circle when $\dim(x_0)$ is 2 and is a ball when $\dim(x_0)$ is 3. Therefore, the 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 $\psi(x)$.

Conclusion and future work. In this study, according to the actual complex system safety requirements, we introduce a fault (an important concept) into the existing CBF-based safety analysis or verification; this can change the operating state of the system or make it abnormal. Furthermore, we propose relevant definitions and mathematical descriptions required for ensuring fault safety. To analyze the system safety after a fault occuring, it is usually necessary to find a function $\psi(x(t)) \in C^r(\chi, R)$ that should satisfy the conditions (3)–(5) in Theorem 1. Under the influence of a fault, it is difficult to guarantee the monotonicity of the system motion trajectory under the mapping $\psi : t \to R$. However, Corollary 1 does not require the mapping $\psi : t \to R$ to remain monotonic and may be suitable for some periodically changing systems. In our future research, we propose to further apply Theorem 2. Our proposed methodology for constructing the barrier function makes the system safety-conservative. Therefore, in future, we have to determine a methodology to construct a new barrier function when there are multiple sets of unsafe states for a system.

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

References

1 Romdlony M Z, Jayawardhana B. Stabilization with guaranteed safety using control Lyapunov-Barrier function. Automatica, 2016, 66: 39–47

2 Prajna S, Rantzer A. On the necessity of barrier certificates. In: Proceedings of the IFAC World Congress, Prague, 2005. 526–531

3 Prajna S, Jadbabaie A, Pappas G J. Stochastic safety verification using barrier certificates. In: Proceedings of the 43rd IEEE Conference on Decision and Control, Nassau, 2004

4 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

5 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

6 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, Chengdu, 2016. 2483–2489

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