Contents lists available at ScienceDirect

Chemical Engineering Research and Design

journal homepage: www.elsevier.com/locate/cherd

Handling bounded and unbounded unsafe sets in Control Lyapunov-Barrier function-based model predictive control of nonlinear processes

Zhe Wu[a], *Panagiotis D. Christofides*[a,b,*]

[a] *Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA*
[b] *Department of Electrical and Computer Engineering, University of California, Los Angeles, CA 90095-1592, USA*

ARTICLE INFO

Article history:
Received 30 November 2018
Received in revised form 29 December 2018
Accepted 2 January 2019
Available online 10 January 2019

Keywords:
Process safety
Process control
Model predictive control
Nonlinear processes

ABSTRACT

Control Lyapunov-Barrier function (CLBF) has been used to design controllers for nonlinear systems subject to input constraints to ensure closed-loop stability and process operational safety simultaneously. In this work, we developed Control Lyapunov-Barrier functions for two types of unsafe regions (i.e., bounded and unbounded sets) to solve the problem of stabilization of nonlinear systems with guaranteed process operational safety. Specifically, in the presence of a bounded unsafe region embedded within the closed-loop system stability region, the CLBF-MPC is developed by incorporating CLBF-based constraints and discontinuous control actions at potential stationary points (except the origin) to guarantee the convergence to the origin (i.e., closed-loop stability) and the avoidance of unsafe region (i.e., process operational safety). In the case of unbounded unsafe sets, closed-loop stability with safety is readily guaranteed under the CLBF-MPC since the origin is the unique stationary point in state-space. The application of the proposed CLBF-MPC method is demonstrated through a chemical process example with a bounded and an unbounded unsafe region, respectively.

1. Introduction

Process operational safety plays an important role in chemical process industries. Unsafe operations can lead to chemical incidents, such as the Chevron refinery fire, 2013 and the ExxonMobil refinery explosion, 2015, in California. It is reported that over 20 chemical incidents occurred in the United States since 2013 (Completed Investigations of Chemical Incidents, 2016), which cause large capital loss, environmental damage and human injuries (Sanders, 2015). Therefore, process operational safety has to be incorporated into control system design such that unsafe operations will be avoided, and the alarm or emergency shut-down system will be triggered automatically instead of relying on human operators. A properly-designed process control system can not only maintain stable production, minimize environmental hazards, and optimize economic profitability, but can also cope with unexpected situations in production that would otherwise result in unsafe operating conditions (Occupational Safety and Health Administration, 2017). However, due to the complexity of chemical processes, an unsafe situation should be understood not simply with respect to a bound on a single measured output (which is used, for example, to activate the elements of the emergency shut-down system), but should also take the interactions between multiple process variables into consideration. Specifically, given a chemical process, the unsafe operating conditions need to be identified in advance based on process knowledge or past industrial data, and con-

* *Corresponding author at:* Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA.
E-mail address: pdc@seas.ucla.edu (P.D. Christofides).
https://doi.org/10.1016/j.cherd.2019.01.002

trol systems should be designed to account for the safe and unsafe operating regions. An example of a metric which characterizes safety in this broader context is a Safeness Index function proposed by Albalawi et al. (2016, 2017) which indicates the relative safeness of each process state accounting for multivariable interactions. Albalawi et al. (2016, 2017) incorporate this Safeness Index state function in a constraint within model predictive control (MPC), an optimization-based control technique, so that the controller regulates the process while accounting for the Safeness Index-based constraints on the process variables.

To maintain the stable and safe operation of a chemical process, model predictive control (MPC), a widely-used advanced control methodology in industrial chemical plants, can be utilized to achieve optimal process performance while accounting for multivariable interactions and limitations of control actuators (Rawlings and Mayne, 2009). Specifically, in Mhaskar et al. (2006), Muñoz de la Peña and Christofides (2008) and Liu et al. (2009), Control Lyapunov function-based constraints were incorporated in MPC to achieve stabilizability within a region of attraction of the closed-loop system (termed the closed-loop system stability region). Additionally, a Safeness Index function was proposed in Albalawi et al. (2017) to account for process operational safety and the corresponding Safeness Index-based constraint (state constraint) was employed in MPC to maintain the process state in a safe operating region in state-space.

More recently, a control method accounting for both stability and safety named Control Lyapunov-Barrier function (CLBF) was proposed in Romdlony and Jayawardhana (2016) and was incorporated in MPC in Wu et al. (2018a,b) such that simultaneous closed-loop stability and process operational safety with recursive feasibility were guaranteed. The CLBF is formulated via the combination (i.e., the weighted average) of a Control Lyapunov function (CLF) and a Control Barrier function (CBF), where CLF is originally used for closed-loop stability and CBF is designed to ensure state constraint adherence. Additionally, another approach to combine CLF and CBF together was proposed in Ames et al. (2017), Jankovic (2018) to utilize quadratic programming to optimize control actions such that both stability and safety objectives are satisfied.

In the direction of CLBF-based MPC developed in Wu et al. (2018a,b), this work investigates the design of CLBF-based controllers for two types of unsafe regions: bounded and unbounded sets. Specifically, it is pointed out in Braun and Kellett (2018) that in the presence of a bounded unsafe region, the origin cannot be rendered asymptotically stable under a continuous CLBF-based control law due to the existence of other stationary points except the origin. Therefore, we study two types of unsafe regions and demonstrate that closed-loop stability and process operational safety can still be achieved for the system with bounded unsafe region if discontinuous control actions are applied at the stationary points. Subsequently, the CLBF-MPC is developed with CLBF-based constraints and is shown to be recursively feasible, and able to drive the closed-loop state to the origin while avoiding the unsafe region at all times if the state originates from a well-defined set of initial conditions.

The rest of the paper is organized as follows: in Section 2, the class of systems considered, the stabilizability assumptions, and the constrained Control Lyapunov-Barrier function developed for two types of unsafe regions (i.e., bounded and unbounded unsafe regions) are given. In Section 3, we introduce the sample-and-hold implementation applied in MPC, and develop a CLBF-based model predictive controller that guarantees recursive feasibility, safety and closed-loop stability under sample-and-hold implementation within an explicitly characterized set of initial conditions. In Section 4, the proposed CLBF-MPC is applied to a nonlinear chemical process example with a bounded and unbounded safe region, respectively, to demonstrate that simultaneous closed-loop stability and process operational safety are achieved under the CLBF-MPC.

2. Preliminaries

2.1. *Notation*

The Euclidean norm of a vector is denoted by the operator $|\cdot|$ and the weighted Euclidean norm of a vector is denoted by the operator $|\cdot|_Q$ where Q is a positive definite matrix. x^T denotes the transpose of x. $\mathbf{R}_+$ denotes the set $[0, \infty)$. The notation $L_fV(x)$ denotes the standard Lie derivative $L_fV(x) := \frac{\partial V(x)}{\partial x} f(x)$. A scalar continuous function $V : \mathbf{R}^n \to \mathbf{R}$ is proper if the set $\{x \in \mathbf{R}^n | V(x) \le k\}$ is compact for all $k \in \mathbf{R}$, or equivalently, V is radially unbounded Malisoff and Mazenc (2009). For given positive real numbers β and ϵ, $\mathcal{B}_\beta(\epsilon) := \{x \in \mathbf{R}^n | |x - \epsilon| < \beta\}$ is an open ball around ϵ with radius of β. The null set is denoted by $\emptyset$. Set subtraction is denoted by "$\setminus$", i.e., $A \setminus B := \{x \in \mathbf{R}^n | x \in A, x \notin B\}$. A function $f(\cdot)$ is of class $\mathcal{C}^1$ if it is continuously differentiable. Given a set $\mathcal{D}$, the boundary and the closure of $\mathcal{D}$ are denoted by $\partial\mathcal{D}$ and $\bar{\mathcal{D}}$, respectively. A continuous function $\alpha : [0, a) \to [0, \infty)$ is said to belong to class $\mathcal{K}$ if it is strictly increasing and is zero only when evaluated at zero.

2.2. *Class of systems*

The class of continuous-time nonlinear systems considered is described by the following state-space form:

$$\dot{x} = f(x) + g(x)u + h(x)w, \quad x(t_0) = x_0 \tag{1}$$

where $x \in \mathbf{R}^n$ is the state vector, $u \in \mathbf{R}^m$ is the manipulated input vector, and $w \in \mathbf{W}$ is the disturbance vector, where $\mathbf{W} := \{w \in \mathbf{R}^l | |w| \le \theta, \theta \ge 0\}$. The control action constraint is defined by $u \in U := \{u_{\min} \le u \le u_{\max}\} \subset \mathbf{R}^m$, where u_{min} and u_{max} represent the minimum and the maximum value vectors of inputs allowed, respectively. $f(\cdot)$, $g(\cdot)$, and $h(\cdot)$ are sufficiently smooth vector and matrix functions of dimensions $n \times 1$, $n \times m$, and $n \times l$, respectively. Without loss of generality, the initial time t_0 is taken to be zero ($t_0 = 0$), and it is assumed that $f(0) = 0$, and thus, the origin is a steady-state of the system of Eq. (1) with $w(t) \equiv 0$, (i.e., $(x_s^*, u_s^*) = (0, 0)$, where x_s^* and u_s^* denote the steady-state of Eq. (1)).

2.3. *Stabilizability assumptions expressed via Lyapunov-based control*

We assume that there exists a positive definite and proper Control Lyapunov function (CLF) V for the nominal system of Eq. (1) with $w(t) \equiv 0$ that satisfies the small control property (i.e., for every $\varepsilon > 0$, $\exists \delta > 0$, s.t. $\forall x \in \mathcal{B}_\delta(0)$, there exists u that satisfies $|u| < \varepsilon$ and $L_fV(x) + L_gV(x)u < 0$, (Sontag, 1989)) and the following condition:

$$L_fV(x) < 0, \quad \forall x \in \{z \in \mathbf{R}^n \setminus \{0\} | L_gV(z) = 0\} \tag{2}$$

The CLF assumption implies that there exists a stabilizing feedback control law $\Phi(x) \in U$ for the nominal system of Eq. (1) (i.e., $w(t) \equiv 0$) that renders the origin of the closed-loop system asymptotically stable for all x in a neighborhood of the origin in the sense that Eq. (2) holds for $u = \Phi(x) \in U$. An example of a feedback control law is given by Lin and Sontag (1991) as follows:

$$k_i(x) = \begin{cases} -\dfrac{p + \sqrt{p^2 + \gamma |q|^4}}{|q|^2} q_i & \text{if} \quad q \neq 0 \\ 0 & \text{if} \quad q = 0 \end{cases} \tag{3a}$$

$$\Phi_i(x) = \begin{cases} u_{\min} & \text{if} \quad k_i(x) < u_{\min} \\ k_i(x) & \text{if} \quad u_{\min} \leq k_i(x) \leq u_{\max} \\ u_{\max} & \text{if} \quad k_i(x) > u_{\max} \end{cases} \tag{3b}$$

where p denotes $L_f V(x)$, q_i denotes $L_{g_i} V(x)$, $q = [q_1 \cdots q_m]^T$, $f = [f_1 \cdots f_n]^T$, $g_i = [g_{i1} \cdots g_{in}]^T$, $(i = 1, 2, \cdots, m)$ and $\gamma > 0$. $k_i(x)$ of Eq. (3a) represents the i_{th} component of the control law $\Phi(x)$ before considering saturation of the control action at the input bounds. $\Phi_i(x)$ of Eq. (3) represents the i_{th} component of the saturated control law $\Phi(x)$ that accounts for the input constraint $u \in U$. Based on the Lyapunov-based control law $\Phi(x)$, a region ϕ_u where the time-derivative of $V(x)$ is negative under the constrained inputs can be characterized: $\phi_u = \{x \in \mathbf{R}^n | \dot{V} < 0, u = \Phi(x) \in U\}$. Additionally, for any initial states $x_0 \in \Omega_b$, where $\Omega_b := \{x \in \phi_u | V(x) \leq b, b > 0\}$ is a level set of $V(x)$ inside ϕ_u, it is guaranteed that $x(t)$, $t \geq 0$ of the nominal system of Eq. (1) with $w(t) \equiv 0$ under $u = \Phi(x) \in U$ remains in the forward invariant set Ω_b.

2.4. *Characterization of unsafe regions*

We assume that there is a set $\lfloor D \subset \mathbf{R}^n$ within which it is unsafe for the system to be operated (e.g., the temperature or pressure is extremely high), and a safe stability region $\lfloor U$ such that $\lfloor U \cap \lfloor D = \emptyset$ and $\{0\} \subset \lfloor U$, within which simultaneous closed-loop stability and process operational safety are achieved in the following sense:

Definition 1. Consider the system of Eq. (1) and input constraints $u \in U$. If there exists a control law $u = \Phi(x) \in U$ such that for any initial state $x(t_0) = x_0 \in \lfloor U$, $x(t)$ remains inside $\lfloor U$, $\forall t \geq 0$, and the origin of the closed-loop system of Eq. (1) can be rendered asymptotically stable, we say that the control law $\Phi(x)$ maintains the process state within a safe stability region $\lfloor U$ at all times.

To ensure process operational safety, the unsafe region $\lfloor D$ should be first characterized by analyzing the safeness of processes based on first-principles models and past operating data. Specifically, the Safeness Index function $S(x)$ proposed in Albalawi et al. (2017) can be utilized to indicate the safeness of a process while accounting for multivariable interactions. From an extensive review of past accidents and their causes, $S(x)$ is developed as a function of process states and the threshold S_{TH} is determined to characterize safe and unsafe regions (i.e., $S(x) \leq S_{TH}$ is safe, and $S(x) > S_{TH}$ is unsafe).

Additionally, in Romdlony and Jayawardhana (2016), Wu et al. (2018a,b), the unsafe region is assumed to be an open, bounded set, and Control Lyapunov-Barrier functions (CLBF)-based control is developed to guarantee closed-loop stability and process operational safety for the system of Eq. (1) for all $x_0 \in \lfloor U$. However, in general, unsafe regions are characterized as unbounded sets in chemical processes, for example, the region where the temperature is above a threshold that can lead to unsafe operations. Therefore, in this work, we will discuss both bounded unsafe region (denoted by $\lfloor D_b$) and unbounded unsafe region (denoted by $\lfloor D_u$) cases and demonstrate that the closed-loop state can be driven to the steady-state and avoid the unsafe region under the CLBF-based controller.

2.5. *Stabilization and safety via Control Lyapunov-Barrier function-based control*

In Romdlony and Jayawardhana (2016), the Control Lyapunov-Barrier function is formulated via the weighted average of a Control Lyapunov function and a Control Barrier function (CBF). Specifically, given a CLF that satisfies Eq. (2) and the small control property, closed-loop stability is achieved under the controller $u = \Phi(x) \in U$. Additionally, CBF is proposed in Wieland and Allgöwer (2007) to ensure process operational safety. The definition of a CBF is given as follows:

Definition 2. Given a set of unsafe points in state-space $\lfloor D$, a $\lfloor C^1$ function $B(x) : \mathbf{R}^n \to \mathbf{R}$ is a CBF if it satisfies the following properties:

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

$$L_f B(x) \leq 0, \quad \forall x \in \{z \in \mathbf{R}^n \backslash \lfloor D | L_g B(z) = 0\} \tag{4b}$$

$$\lfloor X_B := \{x \in \mathbf{R}^n | B(x) \leq 0\} \neq \emptyset \tag{4c}$$

where $\lfloor X_B$ is the safe operating region that excludes $\lfloor D$.

Given the system of Eq. (1) with an unsafe set $\lfloor D$ and a CBF $B(x)$, it is proved in Romdlony and Jayawardhana (2016) that under the feedback controller that satisfies $\dot{B} \leq 0$, it is guaranteed that for all $x_0 \in \lfloor X_B$, the closed-loop state is bounded in $\lfloor X_B$ for all times. Therefore, by combining a CLF and a CBF together, a Control Lyapunov-Barrier function is developed in Romdlony and Jayawardhana (2016) to derive closed-loop stability and process operational safety simultaneously and a constrained CLBF is developed in Wu et al. (2018a,b) to account for the input constraints. The definition of a constrained CLBF is as follows:

Definition 3. Given a set of unsafe points in state-space $\lfloor D$, a proper, lower-bounded and $\lfloor C^1$ function $W_c(x) : \mathbf{R}^n \to \mathbf{R}$ is a constrained CLBF if $W_c(x)$ has a minimum at the origin and also satisfies the following properties:

$$W_c(x) > \rho_c, \quad \forall x \in \lfloor D \subset \phi_{uc} \tag{5a}$$

$$\left|\frac{\partial W_c(x)}{\partial x}\right| \leq r(|x|) \tag{5b}$$

$$L_f W_c(x) < 0, \quad \forall x \in \{z \in \phi_{uc} \backslash (\lfloor D \cup \{0\} \cup \lfloor X_e) | L_g W_c(z) = 0\} \tag{5c}$$

$$\lfloor U_{\rho_c} := \{x \in \phi_{uc} | W_c(x) \leq \rho_c\} \neq \emptyset \tag{5d}$$

where $\rho_c \in \mathbf{R}$, $r(\cdot)$ is a class $\lfloor K$ function, and $\lfloor X_e := \{x \in \phi_{uc} \backslash (\lfloor D \cup \{0\}) | \partial W_c(x)/\partial x = 0\}$ is a set of states where $L_f W_c(x) = 0$ (for $x \neq 0$) due to $\partial W_c(x)/\partial x = 0$.

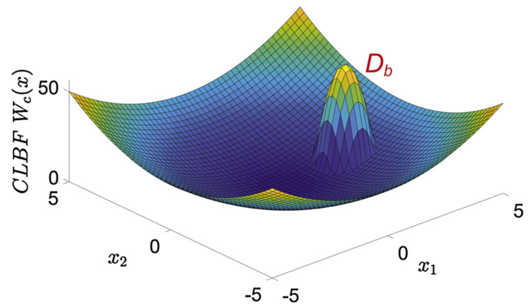

Fig. 1 – A three-dimensional schematic of $W_c(x)$ where the bounded unsafe set $\mathcal{D}_b$ is shown as a mountain peak in the profile of $W_c(x)$ in state-space.

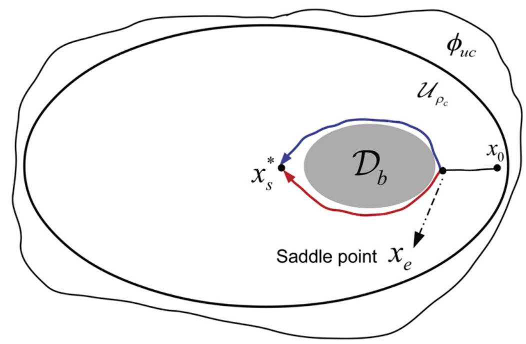

Fig. 2 – A schematic representing a bounded unsafe set $\mathcal{D}_b$ embedded within the stability region, where there exists an initial condition x_0 and a saddle point x_e such that the trajectories from x_0 converge to x_e and pass around $\mathcal{D}_b$ either in the up or down direction with a discontinuous control action at x_e.

Based on the definition of a constrained CLBF $W_c(x)$ of Eq. (5), it is noted that unlike the level sets of Lyapunov functions, the level sets of a constrained CLBF can have negative upper bounds (i.e., $\rho_c < 0$) since $W_c(x)$ is not positive definite. Specifically, the condition of Eq. (5a) defines the unsafe region $\mathcal{D}$. The condition of Eq. (5b) restricts the rate of change of $W_c(x)$ with respect to x, and is used for the sample-and-hold implementation of the controller in Section 3. The condition of Eq. (5c) satisfies the stabilizability assumptions of the CLBF-based controller. Eq. (5d) represents the set of initial conditions $\mathcal{U}_{\rho_c}$. Through the definitions of $\mathcal{D}$ in Eq. (5a) and $\mathcal{U}_{\rho_c}$ in Eq. (5d), it is shown that the set $\mathcal{U}_{\rho_c}$ essentially excludes the unsafe region $\mathcal{D}$ (i.e., $\mathcal{U}_{\rho_c} \cap \mathcal{D} = \emptyset$).

Under a stabilizing control law $\Phi(x)$ (e.g., the Lyapunov-based control law of Eq. (3) with $W_c(x)$ replacing $V(x)$), ϕ_{uc} is defined to be the union of the origin, $\mathcal{X}_e$ and the set where the time-derivative of $W_c(x)$ is negative with constrained input: $\phi_{uc} = \{x \in \mathbf{R}^n | \dot{W}_c = L_f W_c + L_g W_c u < -\alpha |W_c(x) - W_c(0)|,\ u = \Phi(x) \in U\} \cup \{0\} \cup \mathcal{X}_e$, and α is a positive real number used to characterize the set ϕ_{uc}. Consider the nominal system of Eq. (1) (i.e., $w(t) \equiv 0$) with a constrained CLBF $W_c(x)$ of Eq. (5). We analyze closed-loop stability and safety for the following two cases: a bounded unsafe region $\mathcal{D}_b$ and an unbounded unsafe region $\mathcal{D}_u$.

Case 1: If the unsafe region is characterized as a bounded set $\mathcal{D}_b$, it is demonstrated in Braun and Kellett (2018) that asymptotic stability of the origin cannot be achieved under the continuous control law $u = \Phi(x) \in U$ due to the existence of other stationary points (i.e., $x_e \in \mathcal{X}_e$ and $x_e \neq 0$). In other words, for some $x_0 \in \mathcal{U}_{\rho_c}$, the closed-loop state may be trapped in x_e (such stationary points x_e can be either local minima or saddle points of $W_c(x)$) instead of the origin which has the global minimum of $W_c(x)$ under $u = \Phi(x)$. Specifically, as shown in Figs. 1 and 2, since there exist initial values $x_0 \in \mathcal{U}_{\rho_c}$ such that the trajectories from x_0 pass around $\mathcal{D}_b$ in all possible directions, a discontinuous control action has to be applied at x_e to choose a direction to drive the state around $\mathcal{D}_b$ and towards the origin. Moreover, in Wu et al. (2018b), it is noted that in order to escape from x_e and converge to the origin, $W_c(x)$ needs to be carefully designed (e.g., the shapes and functional forms of $V(x)$ and $B(x)$) such that x_e is a saddle point. Since x_e can be characterized once the form of $W_c(x)$ is determined, a set of control actions $\bar{u}$ that can drive the state away from the saddle point in the direction of decreasing $W_c(x)$ should also be calculated in advance and be applied when the closed-loop state converges to x_e.

Following the above analysis, the theorem below provides sufficient conditions under which the existence of a constrained CLBF of Eq. (5) for the system of Eq. (1) under the control law $u = \Phi(x) \in U$ guarantees that the solution of the system of Eq. (1) always stays in the safe stability region $\mathcal{U}_{\rho_c}$. Additionally, besides the boundedness of state in $\mathcal{U}_{\rho_c}$, the origin can be rendered asymptotically stable if discontinuous control actions $\bar{u}$ are applied at saddle points x_e.

Theorem 1. *Consider that a constrained CLBF $W_c(x) : \mathbf{R}^n \to \mathbf{R}$ that has a minimum at the origin and meets the conditions of Eq. (5), exists for the nominal system of Eq. (1) with $w(t) \equiv 0$ subject to input constraints, defined with respect to a bounded unsafe region $\mathcal{D}_b$ in state-space. The continuous feedback control law $u = \Phi(x) \in U$ guarantees that the closed-loop state stays in $\mathcal{U}_{\rho_c}$ for all times for $x_0 \in \mathcal{U}_{\rho_c}$. Additionally, the origin can be rendered asymptotically stable if discontinuous control actions $\bar{u}$ are applied at saddle points x_e.*

Proof. We first prove that the closed-loop state $x(t)$ is bounded in $\mathcal{U}_{\rho_c}$ for all $t \geq 0$, if $x_0 \in \mathcal{U}_{\rho_c}$ and a continuous controller $u = \Phi(x) \in U$ is applied. From the definition of ϕ_{uc} and $\mathcal{X}_e$, $\dot{W}_c$ remains negative (i.e., $\dot{W}_c(x) < -\alpha|W_c(x) - W_c(0)| < 0$) within the set $\phi_{uc} \backslash (\mathcal{X}_e \cup \{0\})$ under the Lyapunov-based control law of Eq. (3) (i.e., $u = \Phi(x) \in U$) with $W_c(x)$ replacing $V(x)$ and in the presence of input constraints. Since $\dot{W}_c = 0$ at $x = x_e \in \mathcal{X}_e, 0$, it holds that $\dot{W}_c \leq 0$ for all $x \in \mathcal{U}_{\rho_c}$. Additionally, since W_c is a proper function and $\dot{W}_c \leq 0$ holds under the controller $u = \Phi(x) \in U$, if follows that the level set $\mathcal{U}_{\rho_c}$ of $W_c(x)$ is a compact invariant set. Therefore, $\forall x_0 \in \mathcal{U}_{\rho_c}$, the state is bounded in the safe stability region $\mathcal{U}_{\rho_c}$ for all times under $u = \Phi(x) \in U$ and does not enter $\mathcal{D}_b$ due to the fact that $\mathcal{U}_{\rho_c} \cap \mathcal{D}_b = \emptyset$. However, asymptotic stability of the origin of the system of Eq. (1) is not guaranteed under the continuous controller $u = \Phi(x) \in U$ since the closed-loop state may converge to x_e instead of the origin. To handle the saddle point issue, discontinuous control actions $\bar{u}$ (i.e., $\bar{u} \neq \Phi(x)$) are required at x_e to drive the state away from x_e. Specifically, if x_e is a saddle point (by a careful design of $W_c(x)$), a path that can escape from the saddle point in the direction of decreasing $W_c(x)$ exists and needs to be determined in advance. Once the state leaves x_e under $\bar{u}$, it is able to move towards the origin under the original controller $u = \Phi(x) \in U$ since $\dot{W}_c$ is negative for all $x \in \mathcal{U}_{\rho_c} \backslash (\mathcal{X}_e \cup \{0\})$. Therefore, the origin which has the global minimum of $W_c(x)$ in $\mathcal{U}_{\rho_c}$ can be rendered asymptotically stable if the closed-loop system of Eq. (1) switches to a discontinuous control action $\bar{u}$ at saddle points x_e. □

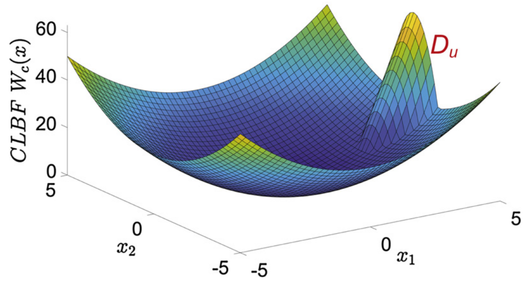

Fig. 3 – A three-dimensional schematic of $W_c(x)$ with an unbounded unsafe set $\lfloor D_u$ in state-space.

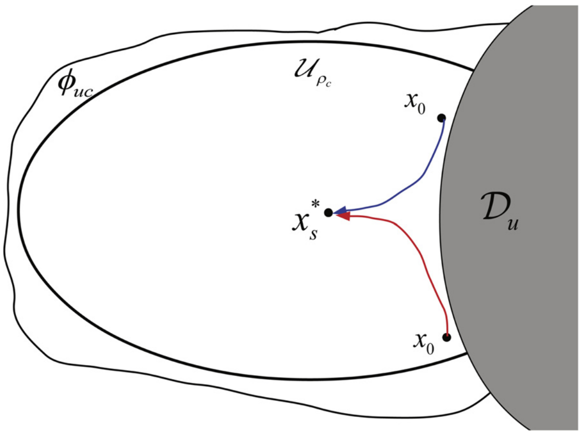

Fig. 4 – A schematic representing an unbounded unsafe set $\lfloor D_u$ in state-space, where the trajectories starting from any initial condition x_0 avoid $\lfloor D_u$ and converge to the origin x_s^*.

Case 2: If an unbounded unsafe region $\lfloor D_u$ is considered, there does not exist such a stationary point $x_e \neq 0$ (Braun and Kellett, 2018), from which the trajectories pass around $\lfloor D_u$ in all directions, which implies that the trajectories from $x_0 \in \lfloor U_{\rho_c}$ converge to the origin while avoiding $\lfloor D_u$ in one direction as shown in Figs. 3 and 4. Therefore, Eq. (5) is simplified with $\lfloor X_e = \emptyset$ and $\dot{W}_c < 0$ holds for all $x \in \lfloor U_{\rho_c} \backslash \{0\}$ under the controller $u = \Phi(x) \in U$. The following theorem demonstrates that closed-loop stability and process operational safety are achieved simultaneously for the system of Eq. (1) under $u = \Phi(x) \in U$.

Theorem 2. *Consider that a constrained CLBF $W_c(x) : \mathbf{R}^n \to \mathbf{R}$ that has a minimum at the origin and meets the conditions of Eq. (5), exists for the nominal system of Eq. (1) with $w(t) \equiv 0$ subject to input constraints, defined with respect to an unbounded unsafe region $\lfloor D_u$ in state-space. The continuous feedback control law $u = \Phi(x) \in U$ guarantees that the closed-loop state is bounded in $\lfloor U_{\rho_c}$ for all times and the origin can be rendered asymptotically stable $\forall x_0 \in \lfloor U_{\rho_c}$.*

Proof. Following the first part of proof for Theorem 1, it is readily shown that $\dot{W}_c$ remains negative for all x in the set $\phi_{uc} \setminus \{0\}$ under the controller $u = \Phi(x) \in U$, which implies that $\forall x_0 \in \lfloor U_{\rho_c} \subset \phi_{uc}$, the state stays in $\lfloor U_{\rho_c}$ for all times and will ultimately converge to the origin due to the fact that $\dot{W}_c < 0, \forall x \in \lfloor U_{\rho_c} \backslash \{0\}$. □

Remark 1. Control Lyapunov-Barrier function $W_c(x)$ and Lyapunov function $V(x)$ are similar in that they both have a global minimum at the origin of state-space and the level sets of $W_c(x)$ and $V(x)$ are both invariant sets. However, the level sets of a CLBF can have negative upper bounds (i.e., $\rho_c < 0$) and there exist multiple stationary points (other than the origin) for $W_c(x)$. Thus, the Lyapunov-based control law (e.g., Sontag control law of Eq. (3) in terms of $V(x)$) guarantees the convergence of the state to the origin (i.e., the equilibrium point at the origin is asymptotically stable), while the CLBF-based control law (e.g., Sontag control law of Eq. (3) in terms of $W_c(x)$) guarantees the boundedness of the state and the avoidance of the unsafe region in a level set of $W_c(x)$. Additionally, the convergence of the state to the origin can be guaranteed for CLBF-based control law if other stationary points (i.e., saddle points) are addressed using a discontinuous control law.

2.6. Design of constrained CLBF

A constrained CLBF can be constructed by following the designing method proposed in Romdlony and Jayawardhana (2016) and Wu et al. (2018a). Specifically, a CLF and a CBF are first designed separately, and a CLBF is designed through the weighted sum of a CLF and a CBF such that the properties in Eq. (5) are satisfied. Proposition 1 provides the guidelines for choosing the CLF and CBF, and the corresponding weights.

Proposition 1. *Given a set $\lfloor D$ of unsafe states (maybe bounded $\mathcal{D}_b$, or unbounded $\mathcal{D}_u$) for the system of Eq. (1) with $w(t) \equiv 0$, assume that there exists a $\lfloor C^1$ CLF $V : \mathbf{R}^n \to \mathbf{R}_+$, and a $\lfloor C^1$ CBF $B : \mathbf{R}^n \to \mathbf{R}$, such that the following conditions hold:*

$$c_1|x|^2 \leq V(x) \leq c_2|x|^2, \quad \forall x \in \mathbf{R}^n, \quad c_2 > c_1 > 0 \tag{6}$$

$$\lfloor D \subset \lfloor H, \quad 0 \not\in \lfloor H \tag{7}$$

$$B(x) = -\eta < 0, \quad \forall x \in \mathbf{R}^n \backslash \lfloor H \tag{8}$$

$$B(x) \geq -\eta, \quad \forall x \in \lfloor H; \quad B(x) > 0, \quad \forall x \in \lfloor D \tag{9}$$

where $\lfloor H$ is a compact set within ϕ_{uc} for bounded unsafe region $\lfloor D_b$ and an unbounded set for unbounded unsafe region $\lfloor D_u$. Define $W_c(x)$ to have the form $W_c(x) := V(x) + \mu B(x) + \nu$, where:

$$\left|\frac{\partial W_c(x)}{\partial x}\right| \leq r(|x|) \tag{10}$$

$$L_f W_c(x) < 0, \quad \forall x \in \{z \in \phi_{uc} \backslash (\lfloor D \cup \{0\} \cup \lfloor X_e) | L_g W_c(z) = 0\} \tag{11}$$

$$\mu > \frac{c_2 c_3 - c_1 c_4}{\eta}, \tag{12a}$$

$$\nu = \rho_c - c_1 c_4, \tag{12b}$$

$$c_3 := \max_{x \in \partial(\lfloor H \cap \phi_{uc})} |x|^2, \tag{12c}$$

$$c_4 := \min_{x \in \partial(\lfloor D \cap \phi_{uc})} |x|^2 \tag{12d}$$

then for initial states $x_0 \in \lfloor U_{\rho_c} \backslash \lfloor D_{\lfloor H}$, where $\lfloor D_{\lfloor H} := \{x \in \lfloor H | W_c(x) > \rho_c\}$, the control law $\Phi(x)$ (with $W_c(x)$ replacing $V(x)$) guarantees that the closed-loop state is bounded in $\lfloor U_{\rho_c}$ and does not enter the unsafe region $\lfloor D_{\lfloor H}$ for all times in the presence of a bounded unsafe region $\lfloor D_b$, and guarantees that the origin is rendered asymptotically stable in the presence of an unbounded unsafe region $\lfloor D_u$.

Remark 2. Following the construction method in Proposition 1, the CLBF $W_c(x)$ satisfies Eq. (5) with an expanded unsafe region $\mathcal{D}_H$ replacing $\mathcal{D}$ and the reader may refer to Wu et al. (2018b) for the detailed proof for the case of a bounded unsafe region $\mathcal{D}_b$. In the presence of an unbounded unsafe region $\mathcal{D}_u$, following the proof in Wu et al. (2018b), it can be readily shown that the control law $u = \Phi(x) \in U$ (with $W_c(x)$ replacing $V(x)$) guarantees that $\forall x_0 \in \mathcal{U}_{\rho_c}$, the closed-loop state is bounded in $\mathcal{U}_{\rho_c}$ and does not enter $\mathcal{D}_u \cap \phi_{uc}$ (i.e., the intersection set of $\mathcal{D}_u$ and ϕ_{uc}), and thus not enter the remaining part of the unbounded unsafe region $\mathcal{D}_u$ for all times by showing that the CLBF $W_c(x)$ satisfies Eq. (5) with an expanded unsafe region $\mathcal{D}_H \cap \phi_{uc}$. Therefore, Theorems 1 and 2 hold for the bounded and unbounded unsafe regions, respectively. Additionally, since the unsafe region $\mathcal{D}$ *(maybe bounded $\mathcal{D}_b$, or unbounded $\mathcal{D}_u$)* is a subset of $\mathcal{D}_H$, it is also guaranteed that the closed-loop state does not enter $\mathcal{D}$ (i.e., closed-loop stability and process operational safety still remain valid for the system of Eq. (1) with an unsafe region $\mathcal{D}$.)

Remark 3. Given a chemical process, the unsafe region $\mathcal{D}$ *(maybe bounded $\mathcal{D}_b$, or unbounded $\mathcal{D}_u$)* can be determined using a Safeness Index function $S(x)$ and its threshold S_{TH} (Albalawi et al., 2017). After the functional form of the unsafe region is achieved (i.e., $\mathcal{D} := \{x \in \mathbf{R}^n | S(x) > S_{TH}\}$), it can be incorporated in the design of $W_c(x)$ following the rules in Proposition 1. It is noted that the construction method for $W_c(x)$ works for any dimension as long as the unsafe region can be characterized as a set in state-space.

3. CLBF-based model predictive control

In this section, a CLBF-based MPC is developed to drive the process state to its steady-state/set-point and avoid the unsafe region by introducing the CLBF-based constraints into MPC. Meanwhile, to handle the potential saddle points due to the bounded unsafe region, another stability constraint is designed to compute a path that drives the state away saddle points and moves towards a smaller level set of $W_c(x)$. Specifically, the impacts of sample-and-hold implementation of the controller and disturbance terms (i.e., $w(t)$ in Eq. (1)) are first discussed. Then the formulation, closed-loop stability and process operational safety of the CLBF-MPC are presented.

3.1. *Sample-and-hold implementation of CLBF-based controller*

The following proposition provides sufficient conditions under which simultaneous closed-loop stability and process operational safety are guaranteed under the sample-and-hold implementation of $u = \Phi(x) \in U$.

Proposition 2. *Consider the system of Eq. (1) with a constrained CLBF W_c that meets the requirements of Definition 3 and has a minimum at the origin. Let $u(t) = \Phi(x(t_k))$ for all $t_k \le t < t_{k+1}$, $x(t_k) \in \mathcal{U}_{\rho_c} \backslash \mathcal{B}_\delta(x_e)$ where $\delta > 0$, $x_e \in \mathcal{X}_e$ and t_k represents the time instance $t = k\Delta$, $k = 0, 1, 2, \ldots$ If $x(t_k) \in \mathcal{B}_\delta(x_e)$, let $u(t) = \bar{u}(x) \in U$ such that $W_c(x(t_{k+1})) < W_c(x(t_k))$ for any $\Delta > 0$. Then, there exists a positive real number Δ^* and real numbers $\rho_s < \rho_{min} < \rho_c$, such that, if $\Delta \in (0, \Delta^*]$ and $x_0 \in \mathcal{U}_{\rho_c}$, then $x(t) \in \mathcal{U}_{\rho_c}$, $\forall t \ge 0$, and $\lim_{t\to\infty} W_c(x(t)) \le \rho_{min}$, where ρ_{min} is determined as follows:*

$$\rho_{min} = \max_{\Delta t \in [0,\Delta^*)} \{W_c(x(t_k + \Delta t), u, w) | x(t_k) \in \mathcal{U}_{\rho_s}, \; u \in U, |w| \le \theta\}. \tag{13}$$

Proof. We mainly discuss the case of a bounded unsafe region with a nonempty set $\mathcal{X}_e$ and show that it also holds for an unbounded unsafe region with $\mathcal{X}_e = \emptyset$. We first show that with $u(t) = u(t_k) = \Phi(x(t_k))$, $\dot{W}_c(x(t), u(t)) < -\epsilon$ holds for all $x(t_k) \in Z := \mathcal{U}_{\rho_c} \backslash (\mathcal{U}_{\rho_s} \cup \mathcal{B}_\delta(x_e))$ and $t \in [t_k, t_k + \Delta^*)$. Since $f(\cdot)$, $g(\cdot)$ and $h(\cdot)$ are smooth functions and $W_c(x)$ satisfies Eq. (5b), following the proof of sample-and-hold implementation of the controller in Wu et al. (2018a), $\dot{W}_c < -\epsilon$ is derived as below:

$$\begin{aligned}\dot{W}_c(x(t), u(t)) &\le \dot{W}_c(x(t_k), u(t_k)) + k_4(k_1 + k_2 + k_3)\Delta^* \\ &< -\alpha\rho_m + k_4(k_1 + k_2 + k_3)\Delta^* \\ &< -\epsilon\end{aligned} \tag{14}$$

where k_1, k_2 and k_3 are Lipschitz constants for $|(L_f W_c(x(t)) - L_f W_c(x(t_k))|$, $|(L_g W_c(x(t)) - L_g W_c(x(t_k)))u(t))|$ and $|(L_h W_c(x(t)) - L_h W_c(x(t_k))|$, respectively, $\rho_m := \min_{x \in \mathcal{Z}} |W_c(x) - W_c(0)|$, and α is a parameter used to characterize ϕ_{uc}. Additionally, since the set Z is bounded, k_4 is determined such that $|x(t) - x(t_k)| \le k_4\Delta^*$ for all $t \in [t_k, t_k + \Delta^*)$. Let $\Delta^* < \frac{\alpha\rho_m - \epsilon}{k_4(k_1 + k_2 + k_3\theta)}$ and $0 \le \epsilon < \alpha\rho_m$, respectively. Therefore, with sufficiently small Δ^* and θ, the sample-and-hold implementation of the controller $u = \Phi(x) \in U$ still maintains $\dot{W}_c$ negative for all $x \in Z$ within each sampling period in the presence of disturbance. Additionally, if $x(t_k) \in \mathcal{B}_\delta(x_e)$ where x_e are saddle points through the design of $W_c(x)$, there also exists a set of control actions $\bar{u}(x)$ that decreases $W_c(x)$ within one sampling period, which implies that $x(t_{k+1})$ moves to a smaller level set of $W_c(x)$. Within finite sampling steps, the state will leave $\mathcal{B}_\delta(x_e)$ and the condition $W_c(x(t)) < W_c(x(t_k))$, $\forall t > t_k$ under $u = \Phi(x) \in U$ ensures that it never returns to $\mathcal{B}_\delta(x_e)$ once it leaves. So far, we prove that the controller (i.e., $u = \Phi(x)$ and $\bar{u}$) in sample-and-hold fashion decreases $W_c(x)$ and drives the state towards $\mathcal{U}_{\rho_s}$.

It remains to show that $x(t)$ will ultimately enter and stay in $\mathcal{U}_{\rho_{min}}$. Since $\dot{W}_c < -\epsilon$, it follows that $W_c(x(t)) < W_c(x(t_k)) \le \rho_c$, $\forall t > t_k$ and thus, within finite sampling steps, the closed-loop state trajectory $x(t)$ will enter $\mathcal{U}_{\rho_s}$. Based on the definition of ρ_{min} of Eq. (13), $x(t)$ stays in $\mathcal{U}_{\rho_{min}}$ for $t \in [t_k, t_k + \Delta^*)$ if $x(t_k) \in \mathcal{U}_{\rho_s}$. Therefore, $\forall x_0 \in \mathcal{U}_{\rho_c}$, the state is bounded in $\mathcal{U}_{\rho_c}$ for all times and ultimately converges to $\mathcal{U}_{\rho_{min}}$.

In case the unsafe region is unbounded, then the origin is the only stationary point in state-space. Therefore, the condition $\dot{W}_c < -\epsilon$ holds for all $x \in \mathcal{U}_{\rho_c} \backslash \mathcal{U}_{\rho_s}$ under the sample-and-hold implementation of $u = \Phi(x) \in U$, which implies that the state will move towards the origin and finally remains inside $\mathcal{U}_{\rho_{min}}$ as well. □

3.2. *Formulation of CLBF-MPC*

The CLBF-MPC design is represented by the following optimization problem:

$$\mathcal{J} = \min_{u \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), \quad u(t))dt \tag{15a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{15b}$$

$$u(t) \in U, \quad \forall t \in [t_k, t_{k+N}) \tag{15c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{15d}$$

$$\dot{W}_c(x(t_k)) < -\epsilon, \quad \text{if } W_c(x(t_k)) > \rho_{\min} \text{ and } x(t_k) \notin B_\delta(x_e) \tag{15e}$$

$$W_c(\tilde{x}(t)) \leq \rho_{\min}, \quad \forall t \in [t_k, t_{k+N}), \quad \text{if } W_c(x(t_k)) \leq \rho_{\min} \tag{15f}$$

$$W_c(\tilde{x}(t)) < W_c(x(t_k)), \quad \forall t \in (t_k, t_{k+N}), \quad \text{if } x(t_k) \in B_\delta(x_e) \tag{15g}$$

where $\tilde{x}(t)$ is the predicted state trajectory, $S(\Delta)$ is the set of piecewise constant functions with period Δ, and N is the number of sampling periods in the prediction horizon. The cost function $L(\tilde{x}(t), u(t))$ is in a quadratic form: $|\tilde{x}(t)|^2_{Q_L} + |u(t)|^2_{R_L}$ where Q_L and R_L are positive definite matrices. The minimum value of the cost function will be attained at the equilibrium of the system of Eq. (1).

In the optimization problem of Eq. (15), the objective function of Eq. (15a) is the integral of $L(\tilde{x}(t), u(t))$ over the prediction horizon. The constraint of Eq. (15b) is the nominal system of Eq. (1) (i.e., $w(t) \equiv 0$) and is used to predict the evolution of the closed-loop state. Eq. (15c) defines the input constraints over the entire prediction horizon. Eq. (15d) defines the initial condition of the nominal process system of Eq. (15b). The constraint of Eq. (15e) forces the CLBF $W_c(\tilde{x})$ along the predicted state trajectories to decrease at least at the rate of $-\epsilon$ when $W_c(x(t_k)) > \rho_{min}$ and $x(t_k) \notin B_\delta(x_e)$, while the constraint of Eq. (15f) activates if $W_c(x(t_k)) \leq \rho_{min}$ so that the states of the closed-loop system will remain inside $U_{\rho_{\min}}$ afterwards. Additionally, if $x(t_k) \in B_\delta(x_e)$, the constraint of Eq. (15g) is activated to decrease $W_c(x)$ within one sampling period such that the state can escape from saddle points x_e. We assume that the states of the closed-loop system are measured at each sampling time. After the optimal solution $u^*(t)$ of the optimization problem of Eq. (15) is obtained, only the first control action of $u^*(t)$ is sent to the control actuators to be applied over the next sampling period. Then, at the next instance of time $t_{k+1} := t_k + \Delta$, the optimization problem is solved again, and the horizon will be rolled forward one sampling time.

Theorem 3 establishes that under the CLBF-MPC of Eq. (15), it is guaranteed that the state of the closed-loop system of Eq. (1) is bounded in U_{ρ_c} for all times, and is ultimately bounded in $U_{\rho_{\min}}$.

Theorem 3. *Consider the system of Eq. (1) with a constrained CLBF W_c which has a minimum at the origin. Given any initial state $x_0 \in U_{\rho_c}$, it is guaranteed that the optimization problem is feasible for all times under the CLBF-MPC scheme of Eq. (15) with sampling period $\Delta \in (0, \Delta^*]$. Additionally, for any $x_0 \in U_{\rho_c}$, the state is bounded in U_{ρ_c}, $\forall t \geq 0$, and ultimately converges to $U_{\rho_{\min}}$ as $t \to \infty$.*

Proof. We first prove that Theorem 3 holds for the bounded unsafe region D_b. Assuming that $x(t_k) \in U_{\rho_c} \backslash U_{\rho_{\min}}$, it is demonstrated in Proposition 2 that in the presence of saddle points x_e, the control law $u = \Phi(x) \in U$ and $u = \bar{u}(x) \in U$ in sample-and-hold fashion are feasible solutions to the optimization problem of Eq. (15) (i.e., guaranteed recursive feasibility of the optimization problem of Eq. (15)) and ensure the decrease of W_c in every sampling period. Specifically, when $x(t_k) \in U_{\rho_c} \backslash (U_{\rho_{\min}} \cup B_\delta(x_e))$, it follows from Eq. (14) that $u = \Phi(x) \in U$ satisfies the constraint of Eq. (15e) because the state is inside the safe stability region $U_{\rho_c} \subset \phi_{uc}$ where there always exists a feasible control action that satisfies $\dot{W}_c < -\epsilon$ according to the definition of ϕ_{uc} (i.e., $\phi_{uc} = \{x \in \mathbf{R}^n | \dot{W}_c = L_f W_c + L_g W_c u < -\alpha |W_c(x) - W_c(0)|, u = \Phi(x) \in U\} \cup \{0\} \cup X_e$). If $x(t_k) \in B_\delta(x_e)$, $u = \bar{u}(x)$ is a feasible solution that satisfies the constraint of Eq. (15g) such that the state of the closed-loop system of Eq. (1) can escape from saddle points x_e and pass around D_b in a specified direction. Additionally, when $x(t_k) \in U_{\rho_{\min}}$, $u = \Phi(x) \in U$ again provides a feasible solution that meets the constraint of Eq. (15f). Therefore, under the constraints of Eqs. (15e–15g), the state of the closed-loop system of Eq. (1) with $x_0 \in U_{\rho_c}$ is first driven towards $U_{\rho_{\min}}$ due to the decrease of $W_c(x)$ while being able to escape from saddle point if the state enters $B_\delta(x_e)$, and ultimately remains inside $U_{\rho_{\min}}$.

On the other hand, if the unsafe region is an unbounded set D_u in state-space, if follows that the origin is the only stationary point in state-space (i.e., $X_e = \emptyset$) and the constraint of Eq. (15g) will never be activated. Therefore, under the constraint of Eq. (15e) (satisfied by a feasible solution $u = \Phi(x) \in U$), $\dot{W}_c$ is rendered negative and the state of the closed-loop system of Eq. (1) is driven towards $U_{\rho_{\min}}$. Finally, the closed-loop state is bounded in $U_{\rho_{\min}}$ under the constraint of Eq. (15f). □

Remark 4. In Theorem 3, we have proved that if $x_0 \in U_{\rho_c}$, $x(t)$ stays inside U_{ρ_c}, $\forall t \geq 0$. Furthermore, we can show that the closed-loop state trajectory of $x(t)$ will always be away from the unsafe region D (maybe bounded $\mathcal{D}_b$, or unbounded $\mathcal{D}_u$) with the application of the CLBF-MPC of Eq. (15). This statement can be proved due to the fact that $x(t) \in U_{\rho_c}$ implies $x(t) \notin D$ for all times since $U_{\rho_c} \cap D = \emptyset$. Also, it can be readily shown that Theorem 3 holds for any subset $U_\rho \subseteq U_{\rho_c}$, i.e., for $x_0 \in U_\rho$, $x(t) \in U_\rho$, $\forall t \geq 0$, and $\limsup_{t\to\infty} |x(t)| \leq d$ following the above proof with U_ρ replacing U_{ρ_c}.

Remark 5. Although the saddle point x_e is a problem for the CLBF-based continuous controller (i.e., $u = \Phi(x) \in U$) in the presence of a bounded unsafe region, it may be mitigated by taking advantage of the MPC layer, within which the objective function of Eq. (15a) and the constraint of Eq. (15g) play an important role. Specifically, since the objective function becomes large if the state converges to any stationary points x_e other than the origin, the optimization problem of Eq. (15) attempts to avoid those sub-optimal points by optimizing control actions in a sample-and-hold fashion and taking future cost values into account. Additionally, the constraint of Eq. (15g) is included in the CLBF-MPC of Eq. (15) such that $W_c(x)$ is forced to decrease if $x(t_k) \in B_\delta(x_e)$. As a result, the state can leave $B_\delta(x_e)$ in the direction of decreasing $W_c(x)$ and keep moving towards the origin.

Remark 6. In the presence of sufficiently small bounded disturbances, closed-loop stability for the system of Eq. (1) under CLBF-MPC is still guaranteed since the disturbances have been accounted for in the sample-and-hold implementation of the controller. Specifically, it is shown in Eq. (13) that once the state enters a small neighborhood around the origin U_{ρ_s}, it will never leave $U_{\rho_{\min}}$ thereafter. In Eq. (14), it is shown that $\dot{W}_c$ can still be rendered negative in the presence of sufficiently small bounded disturbances. Therefore, the closed-loop state will be driven towards the origin under CLBF-MPC (due to the constraint of Eq. (15e)) and ultimately be bounded in $U_{\rho_{\min}}$ (due to the constraint of Eq. (15f)).

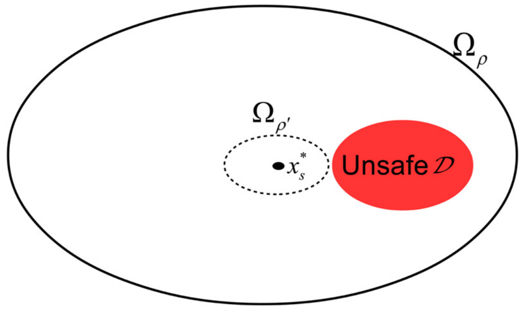

Fig. 5 – A schematic representing a bounded unsafe set $\lfloor D$ in state-space and a conservative safety level set $\Omega_{\rho'}$ inside the closed-loop stability region Ω_ρ.

Remark 7. Note that there also exist other approaches to incorporating process operational safety in the design of MPC. For example, a safety level set of Lyapunov function $\Omega_{\rho'} := \{x \in \phi_u | V(x) \le \rho', \rho' > 0\}$ inside the closed-loop system stability region Ω_ρ can be characterized to exclude the unsafe region (i.e., $\Omega_{\rho'} \cap \lfloor D = \emptyset$) such that for any initial state $x_0 \in \Omega_{\rho'}$, it is guaranteed that the closed-loop state under Lyapunov-based MPC (Mhaskar et al., 2006; Heidarinejad et al., 2012) stays in $\Omega_{\rho'}$ for all times and therefore does not enter $\lfloor D$. Additionally, recursive feasibility of the MPC controller is ensured since the safety level set $\Omega_{\rho'}$ is an invariant set inside ϕ_u where a feasible control action always exists (e.g., the controller $\Phi(x)$ of Eq. (3) with $V(x)$). However, as shown in Fig. 5, considering the location of the unsafe region, the safety level set $\Omega_{\rho'}$ could be very conservative to ensure process operational safety, which limits the operating region and sacrifices process economic performance. On the other hand, the state constraints (i.e., $\tilde{x}(t)$ /in$\lfloor D, \forall t \in [t_k, t_{k+N})$, if $x(t_k)$ /in$\lfloor D$) can be employed in the formulation of MPC to avoid the unsafe region while driving the state towards the origin. In this case, the closed-loop operating region $\Omega_\rho \backslash \lfloor D$ is larger than the conservative safety level set $\Omega_{\rho'}$ in Fig. 5. However, the optimization problem of MPC may become infeasible due to the state constraints when the state approaches the unsafe region, which eventually leads to the failure of control system.

Remark 8. The safety region being bounded or unbounded will not make such a big difference for economic model predictive controller (EMPC) (Wu et al., 2018b). The reason is that EMPC operates the closed-loop system in a time-varying operation by maximizing its economic stage function instead of driving the closed-loop state to the origin. Therefore, we do not need to apply a discontinuous control law around stationary points other than the origin (i.e., saddle points) for a bounded unsafe region, which implies that both bounded and unbounded unsafe regions can be incorporated readily in the design of $W_c(x)$ for EMPC.

4. Application to a chemical process example

In this section, we utilize a chemical process example to illustrate the application of the proposed CLBF-MPC method for both bounded unsafe region $\lfloor D_b$ and unbounded unsafe region $\lfloor D_u$. Consider a well-mixed, non-isothermal continuous stirred tank reactor (CSTR) where an irreversible first-order exothermic reaction takes place. The reaction converts the reactant A to the product B via the chemical reaction $A \rightarrow B$. A heating jacket that supplies or removes heat from the reactor is used. The CSTR dynamic model derived from material and energy balances is given below:

Table 1 – Parameter values of the CSTR.

$T_0 = 310\,K$	$F = 100 \times 10^{-3}\,m^3/min$
$V_L = 0.1\,m^3$	$E = 8.314 \times 10^4\,kJ/kmol$
$k_0 = 72 \times 10^9\,min^{-1}$	$\Delta H = -4.78 \times 10^4\,kJ/kmol$
$C_p = 0.239\,kJ/(kg\,K)$	$R = 8.314\,kJ/(kmol\,K)$
$\rho_L = 1000\,kg/m^3$	$C_{A0_s} = 1.0\,kmol/m^3$
$Q_s = 0.0\,kJ/min$	$C_{A_s} = 0.57\,kmol/m^3$
$T_s = 395.3\,K$	

$$\frac{dC_A}{dt} = \frac{F}{V_L}(C_{A0} - C_A) - k_0 e^{-E/RT} C_A \quad (16a)$$

$$\frac{dT}{dt} = \frac{F}{V_L}(T_0 - T) - \frac{\Delta H k_0}{\rho_L C_p} e^{-E/RT} C_A + \frac{Q}{\rho_L C_p V_L} \quad (16b)$$

where C_A is the concentration of reactant A in the reactor, T is the temperature of the reactor, Q denotes the heat supply/removal rate, and V_L is the volume of the reacting liquid in the reactor. The feed to the reactor contains the reactant A at a concentration C_{A0}, temperature T_0, and volumetric flow rate F. The liquid has a constant density of ρ_L and a heat capacity of C_p. k_0, E and ΔH are the reaction pre-exponential factor, activation energy and the enthalpy of the reaction, respectively. Process parameter values are listed in Table 1. The control objective is to operate the CSTR at the unstable equilibrium point $(C_{As}, T_s) = (0.57\,kmol/m^3, 395.3\,K)$ and maintain the state in a safe region of state-space by manipulating the heat input rate $\Delta Q = Q - Q_s$, and the inlet concentration of species A, $\Delta C_{A0} = C_{A0} - C_{A0_s}$. The input constraints for ΔQ and ΔC_{A0} are $|\Delta Q| \le 0.0167$ kJ/min and $|\Delta C_{A0}| \le 1\,kmol/m^3$, respectively.

We first use deviation variables to represent the process model of Eq. (16) in the form of nonlinear systems of Eq. (1). The equilibrium point (C_{As}, T_s) is at the origin of the state-space. $x^T = [C_A - C_{As} T - T_s]$, $u^T = [\Delta C_{A0} \Delta Q]$ represent the state vector and the manipulated input vector in deviation variable form, respectively. The Control Lyapunov Function is designed using the standard quadratic form $V(x) = x^T P x$, with the following positive definite P matrix:

$$P = \begin{bmatrix} 9.35 & 0.41 \\ 0.41 & 0.02 \end{bmatrix} \quad (17)$$

We first demonstrate the application of the proposed CLBF-MPC control scheme to a bounded unsafe region $\lfloor D_b$ located within the set ϕ_{uc}. The unsafe region is defined as an ellipse:

$$D_b := \left\{ x \in \mathbf{R}^2 | F(x) = \frac{(x_1 + 0.22)^2}{1} + \frac{(x_2 - 4.6)^2}{1 \times 10^4} < 2 \times 10^{-4}. \right\}$$

$\lfloor H$ is defined as $\lfloor H := \{x \in \mathbf{R}^2 | F(x) < 4 \times 10^{-4}\}$ such that it satisfies $D_b \subset \lfloor H$ in Proposition 1. The Control Barrier function $B(x)$ is defined as follows.

$$B(x) = \begin{cases} e^{\frac{aF^2(x)}{F(x) - 4 \times 10^{-4}}} - e^{-2a \times 10^{-4}}, & \text{if } x \in \lfloor H \\ -e^{-2a \times 10^{-4}}, & \text{if } x \text{ /in} \lfloor H \end{cases} \quad (18)$$

where a is a parameter that can be adjusted in characterizing the set ϕ_{uc}. The Control Lyapunov-Barrier function $W_c(x) = V(x) + \mu B(x) + \nu$ is constructed following the rules in Proposition 1, where the parameter values can be found in

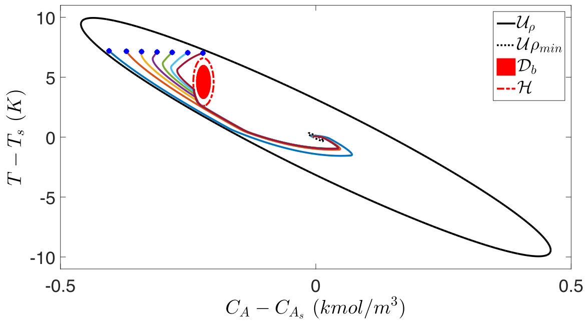

Fig. 6 – Closed-loop state trajectories under the CLBF-MPC for the system of Eq. (16) with different initial conditions marked by stars. The set of unsafe states $\lfloor D_b$ is shaded in solid red area and the set $\lfloor U_\rho$ is the region between the level set of the Lyapunov function and the set $\lfloor H$.

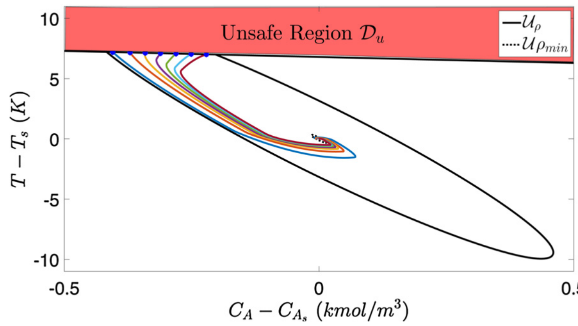

Fig. 7 – Closed-loop state trajectories under the CLBF-MPC for the system of Eq. (16) with different initial conditions marked by stars. The set of unbounded unsafe states $\lfloor D_u$ is the red area on the top.

Wu et al. (2018a). In this example, x_e is calculated to be (−0.235, 4.83), which is a saddle point in state-space.

The objective function of the CLBF-MPC in this example is give by $\int_{t_k}^{t_{k+N}} |\tilde{x}(t)|^2_{Q_L} + |u(t)|^2_{R_L}$, where the weighting matrices for the states and inputs are chosen to be $Q_L = \begin{bmatrix} 1000 & 0 \\ 0 & 10 \end{bmatrix}$ and $R_L = \begin{bmatrix} 1 & 0 \\ 0 & 100 \end{bmatrix}$, respectively. In the simulations presented below, the explicit Euler method with an integration time step of $h_c = 10^{-5}$ min is used to numerically integrate the process model of Eq. (16). The MPC sampling time is $\Delta = 2\times 10^{-3}$ min and the prediction horizon is $N = 10$. In Fig. 6, it is demonstrated that for all initial states x_0 in $\lfloor U_\rho$ (marked by blue stars), which is a subset of $\lfloor U_{\rho_c}$, the closed-loop state avoids the bounded unsafe region $\lfloor D_b$ and ultimately converges to $\lfloor U_{\rho_{\min}}$ under the CLBF-MPC of Eq. (15).

We now study the case where the unsafe region is an unbounded set. The unsafe region is defined as an unbounded set with high temperature and concentration: $\lfloor D_u := \{x \in \mathbf{R}^2 | F(x) = x_1 + x_2 > 7.2\}$. $\lfloor H$ is defined as $\lfloor H := \{x \in \mathbf{R}^2 | F(x) > 6.8\}$.The Control Barrier function $B(x)$ is defined as follows.

$$B(x) = \begin{cases} e^{F(x)-7.2} - 2\times e^{-0.4}, & \text{if } x \in \lfloor H \\ -e^{-0.4}, & \text{if } x \notin \lfloor H \end{cases} \quad (19)$$

The Control Lyapunov-Barrier function $W_c(x) = V(x) + \mu B(x) + \nu$ is constructed with the following parameters: $\rho_c = 0$, $c_1 = 0.001$, $c_2 = 10$, $c_3 = 98.78$, $c_4 = 51.99$, and $\nu = \rho_c - c_1 c_4 = -1.685\times 10^{-2}$. Hence, μ is chosen to be 1500 to satisfy Eq. (12). It is demonstrated in Fig. 7 that under the CLBF-MPC of Eq. (15), all the trajectories with initial states inside $\lfloor U_\rho$ avoid the unsafe region $\lfloor D_u$ on the top and converge to $\lfloor U_{\rho_{\min}}$.

Therefore from the above case studies of a bounded and an unbounded unsafe region, it is demonstrated that simultaneous closed-loop stability and process operational safety are achieved under the CLBF-MPC of Eq. (15) in the sense that for any initial state $x_0 \in \lfloor U_\rho \subset \lfloor U_{\rho_c}$, the closed-loop state is guaranteed to stay inside $\lfloor U_\rho$ and avoid the unsafe region for all times, and will converge to a small neighborhood $\lfloor U_{\rho_{\min}}$ around the origin ultimately.

5. Conclusion

In this work, we investigated simultaneous closed-loop stability and process operational safety of nonlinear systems subject to input constraints under the CLBF-based model predictive control scheme for two types of unsafe regions (i.e., bounded and unbounded sets). Specifically, in the presence of a bounded unsafe region, to avoid the convergence to other stationary points except the origin in state-space, discontinuous control actions were required at stationary points (other than the origin) to drive the state away from the stationary points and towards the origin. However, if an unbounded unsafe region was considered, then the origin could be rendered asymptotically stable under a continuous feedback control law since there are no stationary points present in this case. As a result, in developing the CLBF-based model predictive control scheme, an additional constraint was added to handle stationary points in the presence of a bounded unsafe region which is embedded within the closed-loop system stability region. Finally, a chemical process example was utilized to demonstrate the application of CLBF-MPC to a CSTR system with bounded and unbounded unsafe regions.

Acknowledgment

Financial support from the National Science Foundation and the Department of Energy is gratefully acknowledged.

References

Albalawi, F., Alanqar, A., Durand, H., Christofides, P.D., 2016. A feedback control framework for safe and economically-optimal operation of nonlinear processes. AIChE J. 62, 2391–2409.

Albalawi, F., Durand, H., Christofides, P.D., 2017. Process operational safety using model predictive control based on a process safeness index. Comput. Chem. Eng. 104, 76–88.

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

Braun, P., Kellett, C.M., 2018. On (the existence of) control Lyapunov Barrier functions. Preprint, https://eref.uni-bayreuth.de/40899.

Completed Investigations of Chemical Incidents, 2016. Final Report of the Investigations of Chemical Incidents, Technical Report. U.S. Chemical Safety and Hazard Investigation Board.

Jankovic, M., 2018. Robust control barrier functions for constrained stabilization of nonlinear systems. Automatica 96, 359–367.

Heidarinejad, M., Liu, J., Christofides, P.D., 2012. Economic model predictive control of nonlinear process systems using Lyapunov techniques. AIChE J. 58, 855–870.
Lin, Y., Sontag, E.D., 1991. A universal formula for stabilization with bounded controls. Syst. Control Lett. 16, 393–397.
Liu, J., Muñoz de la Peña, D., Christofides, P.D., Davis, J.F., 2009. Lyapunov-based model predictive control of nonlinear systems subject to time-varying measurement delays. Int. J. Adapt. Control Signal Process. 23, 788–807.
Malisoff, M., Mazenc, F., 2009. Constructions of Strict Lyapunov Functions. Springer Science & Business Media.
Mhaskar, P., El-Farra, N.H., Christofides, P.D., 2006. Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. Syst. Control Lett. 55, 650–659.
Muñoz de la Peña, D., Christofides, P.D., 2008. Lyapunov-based model predictive control of nonlinear systems subject to data losses. IEEE Trans. Autom. Control 53, 2076–2089.
Occupational Safety & Health Administration, 2017. OSHA 29 CFR 1910.119. Technical Report. Process Safety Management of Highly Hazardous Chemicals.
Rawlings, J.B., Mayne, D.Q., 2009. Model Predictive Control: Theory and Design. Nob Hill Pub.
Romdlony, M.Z., Jayawardhana, B., 2016. Stabilization with guaranteed safety using control Lyapunov-Barrier function. Automatica 66, 39–47.
Sanders, R.E., 2015. Chemical Process Safety: Learning from Case Histories. Butterworth-Heinemann.
Sontag, E.D., 1989. A ‘universal’ construction of Artstein’s theorem on nonlinear stabilization. Syst. Control Lett. 13, 117–123.
Wieland, P., Allgöwer, F., 2007. Constructive safety using control barrier functions. IFAC Proc. Vol. 40, 462–467.
Wu, Z., Albalawi, F., Zhang, Z., Zhang, J., Durand, H., Christofides, P.D., 2018a. Control Lyapunov-Barrier function-based model, predictive control of nonlinear systems. In: Proceedings of the American Control Conference, Milwaukee, Wisconsin, pp. 5920–5926.
Wu, Z., Durand, H., Christofides, P.D., 2018b. Safe economic model predictive control of nonlinear systems. Syst. Control Lett. 118, 69–76.