Computers and Chemical Engineering 159 (2022) 107690

Contents lists available at ScienceDirect

Computers and Chemical Engineering

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

Barrier-function-based distributed predictive control for operational safety of nonlinear processes

Scarlett Chen[a], Zhe Wu[c], 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
[c] Department of Chemical and Biomolecular Engineering, National University of Singapore, 117585, Singapore

ARTICLE INFO

Article history:
Received 6 December 2021
Revised 20 January 2022
Accepted 22 January 2022
Available online 25 January 2022

Keywords:
Distributed control
Process operational safety
Barrier function
Model predictive control
Nonlinear systems

ABSTRACT

This article focuses on the design of distributed model predictive control (DMPC) systems for nonlinear processes with input constraints using a Control Lyapunov-Barrier Function (CLBF) to achieve simultaneous closed-loop stability and process safety. Specifically, we first use a constrained CLBF to design explicit control laws for each subsystem and to characterize a set of initial conditions, starting from which the closed-loop states of the overall nonlinear system are guaranteed to converge to the operating steady-state under the CLBF-based control laws while avoiding unsafe regions in state space. We then propose the CLBF-based DMPC, and prove its feasibility and effectiveness in ensuring the stability and avoidance of unsafe regions under sample-and-hold implementation of DMPC control actions. The CLBF-based DMPC is applied to both sequential and iterative DMPC designs in the general sense, and a modification to the DMPC formulation is presented for special cases of systems where the coupling between subsystems is in a one-way cascading manner. The proposed CLBF-DMPC method is demonstrated via a nonlinear chemical process example consisting of two subsystems.

1. Introduction

Process safety is inarguably a top priority in industrial engineering given the involvement of operators with potential hazards and exposure to the environment. During each stage of design, operation, and maintenance, risk assessment and analysis is an irreplaceable part of engineering and implementation in order to prevent catastrophic events from happening. Process control systems not only enable automated control, operation, and monitoring of the plant, but also allow safe, stable, and optimal production if robust control designs are implemented. The work in Leveson and Stephanopoulos (2014) provides a control-inspired approach for the engineering of safe processes, and by defining process safety within a system-theoretic framework, allows for a comprehensive treatment of process safety. The interacting dynamics between multiple subsystems of a complex industrial plant and their combined impact on process safety and operations are factors that should be taken into consideration in order to handle and avoid unexpected circumstances and hazards. To this end, a model predictive control (MPC) system stands out as a candidate control method to handle safety constraints, multi-variable interactions, and nonlinearities in large-scale processes (Garcia et al., 1989). In particular, in order to work with large-scale processes that possess large amount of state variables and sensor data, distributed MPC (DMPC) has been proposed to reduce computational time and complexity of the optimization problem (Christofides et al., 2013). In a DMPC framework, collective control objectives are achieved by multiple controllers which have inter-controller communication established to calculate their respective control actions. Previous works on decentralized and distributed MPC systems (Venkat et al., 2004; Stewart et al., 2010; Christofides et al., 2013) have shown the effectiveness of this approach in improving closed-loop performance while reducing computational time; and more recently, they have been used in cases where machine-learning modeling may be adopted (Chen et al., 2020), as well as in applications of demonstrated robustness against cyber-attacks (Chen et al., 2021a). Within a distributed framework, there exist many configuration variants depending on the degree of communication between subcontrollers, and have been applied to various engineering applications such as distributed smart grid optimization, moving horizon estimation of reactor-separator process, and distributed model predictive control of multi-motor driving cutterhead systems

* 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.compchemeng.2022.107690
0098-1354/

(Zhang and Liu, 2013; Qi et al., 2013; Yang et al., 2019). Sequential DMPC allows one-way communication from one controller to the next, while iterative DMPC allows two-way communication between all controllers and iteration during the optimization calculations until a termination criterion has been met. Both of these two frameworks have been used in recent literature (Liu et al., 2010; 2012; Yang et al., 2019) and will be discussed in this work.

Barrier functions, or barrier certificates, serve as an important tool in safety-critical systems where multi-objective control is involved (Xu et al., 2015). To account for safety constraints in a process, control laws based on a Control-Lyapunov-Barrier-Function (CLBF) can be developed and subsequently incorporated in the design of MPC algorithms to ensure stability and safety of operation (Wu et al., 2019). More specifically, CLBFs can be developed by integrating a Control Barrier Function (CBF), which is an extension of barrier functions applied to a controlled system, and a Control Lyapunov function (CLF). While CLFs work to characterize a stability region, CBFs characterize unsafe regions that closed-loop state must not enter during operation (Romdlony and Jayawardhana, 2016). CLBF-MPC has been proposed in Wu et al. (2019); Wu and Christofides (2019), where the stability and safety analysis for the closed-loop system in the presence of both bounded and unbounded unsafe sets have been provided. Many other recent works (Marvi and Kiumarsi, 2021; Zeng et al., 2021) have also explored MPC with discrete-time control barrier functions, as well as optimal control based on reinforcement learning with the inclusion of control barrier functions. In this work, we introduce CLBF to the design of DMPC in controlling multiple subsystems. This contribution is essential to the operation of complex industrial processes where the overall system may encounter regions in state-space for which they would like to avoid, and the sub-controllers for each subsystem need to work cooperatively to achieve the stability and safety objectives. In this work, we use an analytical representation of the unsafe operating points in state-space to specify the CLBFs. However, interested readers may also refer to previous works in Chen et al. (2022) for machine-learning-based methods of characterizing such regions and designing MPC algorithms based on a feedforward-neural-network-based control barrier function. The unsafe operating regions may be specified for each subsystem individually, or if these unsafe points are interdependent across subsystems, the unsafe regions may be specified holistically with respect to the overall process.

The remainder of the paper is organized as follows. We address the class of systems considered, the stabilizability assumptions, and the definition of Control Lyapunov-Barrier Functions in Section 2. In Section 3, we provide the formulation of DMPCs, and develop a CLBF-based DMPCs that guarantee recursive feasibility, closed-loop stability and safety under the sample-and-hold control action implementation for the general case. We also provide a modified DMPC framework for special cases of coupled subsystems in order to demonstrate its advantages and drawbacks. In Section 4, we demonstrate the applicability of the proposed control scheme using a nonlinear chemical process example.

2. Preliminaries

2.1. Notation

We use $|\cdot|$ to denote the Euclidean norm of a vector. x^T denotes the transpose of x. If a function $f(\cdot)$ is continuously differentiable, it is of class $\mathcal{C}^1$. $L_f V(x) := \frac{\partial V(x)}{\partial x} f(x)$ represents the Lie derivative. We say that a continuous scalar function $V : \mathbf{R}^n \to \mathbf{R}$ is a proper function, if the set $\{x \in \mathbf{R}^n \mid V(x) \leq k\}$ is a compact set $\forall\ k \in \mathbf{R}$. With positive real numbers β and ϵ, we use $\mathcal{B}_\beta(\epsilon) := \{x \in \mathbf{R}^n \mid |x - \epsilon| < \beta\}$ to represent an open ball around ϵ with radius of β. $A \backslash B := \{x \in \mathbf{R}^n \mid x \in A, x \notin B\}$ denotes set subtraction.

2.2. Class of systems

A general class of nonlinear systems is considered in which multiple distinct sets of manipulated inputs exist. Each set of inputs regulates a specific subsystem. Throughout the manuscript, we consider two subsystems – subsystem-1 and subsystem-2 – for the simplicity of notation. Subsystem-1 and subsystem-2 consist of states x_1 and x_2 respectively, which are controlled by and only by u_1 and u_2 respectively. The general class of system under consideration can be represented by nonlinear ordinary differential equations as follows:

$$\begin{aligned} &\dot{x} = F(x, u_1, u_2, w) := f(x) + g_1(x)u_1 + g_2(x)u_2 + \nu(x)w, \\ &x(t_0) = x_0 \end{aligned} \tag{1}$$

where $x \in \mathbf{R}^n$ denotes the state vector, $u_1 \in \mathbf{R}^{m_1}$ and $u_2 \in \mathbf{R}^{m_2}$ are the two distinct sets of input vectors, and the disturbance is denoted by $w \in W$ with $W := \{w \in \mathbf{R}^r \mid |w| \leq w_m,\ w_m \geq 0\}$. There are constraints on the control actions as defined by $u_1 \in U_1 := \{u_{1_i}^{\min} \leq u_{1_i} \leq u_{1_i}^{\max}, i = 1, \ldots, m_1\} \subset \mathbf{R}^{m_1}$, and $u_2 \in U_2 := \{u_{2_i}^{\min} \leq u_{2_i} \leq u_{2_i}^{\max}, i = 1, \ldots, m_2\} \subset \mathbf{R}^{m_2}$. $f(\cdot)$, $g_1(\cdot)$, $g_2(\cdot)$, and $\nu(\cdot)$ are matrix and vector functions of dimensions $n \times 1$, $n \times m_1$, $n \times m_2$, and $n \times r$, respectively, which are assumed to be sufficiently smooth. The initial time t_0 is taken to be zero ($t_0 = 0$), and we assume that $f(0) = 0$. Therefore, the origin is an equilibrium point of the nominal system of Eq. (1) with $w(t) \equiv 0$ (i.e., $(x_s, u_{1s}, u_{2s}) = (0, 0, 0)$, where x_s, u_{1s} and u_{2s} represent the steady-state state and input vectors).

2.3. Control Lyapunov function

With the nominal system of Eq. (1) with $w(t) \equiv 0$ in consideration, it is assumed that a Control Lyapunov Function (CLF) V exists, which is positive definite and proper; the CLF meets the small control property, which indicates that for every positive ε, there exists a positive δ, such that $\forall\ x \in \mathcal{B}_\delta(0)$, $\exists\ u^T = [u_1^T,\ u_2^T]$ that meet the conditions of $|u| < \varepsilon$ and $L_f V(x) + L_{g_1} V(x) \cdot u_1 + L_{g_2} V(x) \cdot u_2 < 0$ Sontag (1989). In addition, the CLF also satisfies the following conditions:

$$\begin{aligned} &L_f V(x) < 0, \\ &\forall x \in \{z \in \mathbf{R}^n \backslash \{0\} \mid L_{g_1} V(z) = 0,\ L_{g_2} V(z) = 0\} \end{aligned} \tag{2}$$

The existence of V implies the existence of explicit feedback control laws $\Phi_1(x) \in U_1,\ \Phi_2(x) \in U_2$ such that Eq. (2) holds for the nominal system of Eq. (1) under $u_1 = \Phi_1(x) \in U_1,\ u_2 = \Phi_2(x) \in U_2$, and for all x in an explicitly defined neighborhood around the origin, the closed-loop system is rendered asymptotically stable. The Sontag control law in Lin and Sontag (1991) is one example of such stabilizing feedback control laws. A region ϕ_u can be characterized around the origin where the time derivative of the Lyapunov function $V(x)$ is negative under $u_1 = \Phi_1(x) \in U_1,\ u_2 = \Phi_2(x) \in U_2$ as: $\phi_u = \{x \in \mathbf{R}^n \mid \dot{V}(x) = L_f V(x) + L_{g_1} V(x) \cdot u_1 + L_{g_2} V(x) \cdot u_2 < 0, u_1 = \Phi_1(x) \in U_1,\ u_2 = \Phi_2(x) \in U_2\} \cup \{0\}$. Within ϕ_u, we define $\Omega_b := \{x \in \phi_u \mid V(x) \leq b,\ b > 0\}$, which is a level set of $V(x)$ and a forward invariant set. For the closed-loop system under $u_1 = \Phi_1(x) \in U_1,\ u_2 = \Phi_2(x) \in U_2$, Ω_b is considered as the stability region in the sense that, for any $x_0 \in \Omega_b$, the closed-loop trajectory $x(t),\ t \geq 0$ of the nominal system of Eq. (1) (i.e., $w(t) \equiv 0$) remains in Ω_b.

2.4. Control barrier function

During operation, there are undesirable regions within state-space that must be avoided for safety and/or other considerations related to cost, environment, and optimality. Let us assume that an open set $\mathcal{D}$ exists, and it sufficiently describes the region to be avoided. In the remainder of the manuscript, the notation $\mathcal{D}$

is used to represent the unsafe set. A safe set can be subsequently defined as $\mathcal{X}_0 := \{x \in \mathbf{R}^n \backslash \mathcal{D}\}$ where $\mathcal{X}_0 \cap \mathcal{D} = \emptyset$, $\{0\} \in \mathcal{X}_0$. $\mathcal{X}_0$ will include the set of initial conditions that we consider. Both bounded and unbounded unsafe regions have been studied in literature; in this manuscript, bounded unsafe set is denoted as $\mathcal{D}_b$, unbounded unsafe set is denoted as $\mathcal{D}_u$, respectively.

The definition of process operational safety studied in this manuscript entails closed-loop states not entering any unsafe sets. Formally, operational safety has a definition described as follows:

Definition 1. The nominal system of Eq. (1) under input constraints $u \in U$ and with $w(t) \equiv 0$ is considered. If a set of constrained control actions $u_1 = \Phi_1(x) \in U_1,\ \ u_2 = \Phi_2(x) \in U_2$ exists such that, for any initial state $x(t_0) = x_0 \in \mathcal{X}_0$, the process state trajectories do not enter the unsafe region and converge to the origin asymptotically (i.e., $x(t) \in \mathcal{X}_0$, $x(t) \notin \mathcal{D}$, $\forall\ t \geq 0$), then the control actions $u_1 = \Phi_1(x),\ \ u_2 = \Phi_2(x)$ are able to maintain the closed-loop state within a safe operating region $\mathcal{X}_0$ at all times.

Subsequently, with the introduction of safe and unsafe operating regions in state-space, we can define a valid Control Barrier Function (CBF) in the following definition: Wieland and Allgöwer (2007).

Definition 2. With a set of unsafe points $\mathcal{D}$ in state-space, a $\mathcal{C}^1$ function $B(x) : \mathbf{R}^n \to \mathbf{R}$ is a Control Barrier Function if it satisfies these properties:

$$B(x) > 0, \quad \forall\ x \in \mathcal{D} \tag{3a}$$

$$L_f B(x) \leq 0,\ \ \forall\ x \in \{z \in \mathbf{R}^n \backslash \mathcal{D} \mid L_g B(z) = 0\} \tag{3b}$$

$$\mathcal{X}_B := \{x \in \mathbf{R}^n \mid B(x) \leq 0\} \neq \emptyset \tag{3c}$$

3. Stabilization and safety via control Lyapunov-barrier function

The work in Romdlony and Jayawardhana (2016) proposed a Control Lyapunov-Barrier Function (CLBF) and proved that if a valid CLBF exists for the nominal system of Eq. (1), then for any initial condition $x_0 \in \mathcal{X}_0$, a control law exists which maintains the closed-loop state outside of $\mathcal{D}$ and within an explicitly characterized region around the steady-state (which is a level set of CLBF) at all times. In Wu and Christofides (2019); Wu et al. (2019), this work is extended to including constraints on the manipulated inputs $u \in U$ in the design of CLBFs. In all three works, the CLBF was designed using a weighted sum of a CBF and a CLF, where the CBF satisfies the properties outlined in Eq. (3), and the CLF meets the relevant conditions in Section 2.3. Then, a practical design guideline is presented in Wu et al. (2019) to construct this CLBF. We can reference and utilize the same guidelines, applied on the nonlinear system of Eq. (1) consisting of multiple subsystems to design the CLBF for the overall process.

The definition of a constrained CLBF $W(x)$ with respect to the overall process as represented by the nonlinear model of Eq. (1) is shown as below:

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

$$W(x) > \rho, \quad \forall\ x \in \mathcal{D} \subset \phi_{uc} \tag{4a}$$

$$L_f W(x) < 0,$$
$$\forall\ x \in \{z \in \phi_{uc} \backslash (\mathcal{D} \cup \{0\} \cup \mathcal{X}_e) \mid L_{g_1} W(z) = 0,$$
$$L_{g_2} W(z) = 0\} \tag{4b}$$

$$\mathcal{U}_\rho := \{x \in \phi_{uc} \mid W(x) \leq \rho\} \neq \emptyset \tag{4c}$$

$$\overline{\phi_{uc} \backslash (\mathcal{D} \cup \mathcal{U}_\rho)} \cap \overline{\mathcal{D}} = \emptyset \tag{4d}$$

where $\mathcal{X}_e := \{x \in \phi_{uc} \backslash (\mathcal{D} \cup \{0\}) \mid \frac{\partial W(x)}{\partial x} = 0\}$ represents a set of states where $L_f W(x) = 0$ (for $x \neq 0$) due to $\frac{\partial W(x)}{\partial x} = 0$. $\rho \in \mathbf{R}$ is a real constant. f, g_1, g_2 are the vector and matrix functions from Eq. (1). Using a set of explicit control laws subject to their lower and upper bounds $u_1 = \Phi_1(x) \in U_1,\ \ u_2 = \Phi_2(x) \in U_2$, ϕ_{uc} is defined to be the union of the origin, the set $\mathcal{X}_e$, and the set where the time-derivative of $W(x)$ is negative: $\phi_{uc} = \{0\} \cup \mathcal{X}_e \cup \{x \in \mathbf{R}^n \mid \dot{W}(x(t), \Phi_1(x), \Phi_2(x)) = L_f W + L_{g_1} W \cdot u_1 + L_{g_2} W \cdot u_2 < -\alpha_W |W(x) - W(0)|,\ \ u_1 = \Phi_1(x) \in U_1,\ \ u_2 = \Phi_2(x) \in U_2,\ \ \alpha_W > 0\}$. For the nominal system of Eq. (1) with $w(t) \equiv 0$, if a $\mathcal{C}^1$ constrained CLBF $W(x)$ exists, then there exists a set of control laws $u_1 = \Phi_1(x) \in U_1,\ \ u_2 = \Phi_2(x) \in U_2$ that together render the origin asymptotically stable within ϕ_{uc}. The CLBF function has a minimum at the origin and is able to satisfy the following properties $\forall\ x \in \phi_{uc}$:

$$c_1 |x|^2 \leq W(x) - \rho_0 \leq c_2 |x|^2, \tag{5a}$$

$$\frac{\partial W(x)}{\partial x} F(x, \Phi_1(x), \Phi_2(x)) \leq -c_3 |x|^2,\ \ \forall\ x \in \phi_{uc} \backslash \mathcal{B}_\delta(x_e) \tag{5b}$$

$$\left| \frac{\partial W(x)}{\partial x} \right| \leq c_4 |x| \tag{5c}$$

where $F(x, u_1, u_2)$ is the nominal system of Eq. (1) with $w(t) \equiv 0$, $c_j(\cdot) > 0$, $j = 1,\ 2,\ 3,\ 4$ are real numbers, ρ_0 represents the global minimum of $W(x)$ at the origin (i.e., $W(0) = \rho_0$), and $\mathcal{B}_\delta(x_e)$ denotes a neighborhood surrounding a saddle point in state-space, $x_e \in \mathcal{X}_e$.

Within the nonlinear system described by Eq. (1), the functions f, g_1, g_2 and ν are assumed to be sufficiently smooth, thus positive constants L_x, L_w, L_x', L_w', and M exist (by continuity) s.t. $\forall\ x, x' \in \mathcal{U}_\rho$, $w \in W$, and $u_1 \in U_1,\ \ u_2 \in U_2$, the conditions below will hold:

$$|F(x, u_1, u_2, w)| \leq M \tag{6a}$$

$$|F(x, u_1, u_2, w) - F(x', u_1, u_2, 0)| \leq L_x |x - x'| + L_w |w| \tag{6b}$$

$$\left| \frac{\partial W(x)}{\partial x} F(x, u_1, u_2, w) - \frac{\partial W(x')}{\partial x} F(x', u_1, u_2, 0) \right| \leq L_x' |x - x'| + L_w' |w_m| \tag{6c}$$

Remark 1. When designing local controllers, we could consider designing a CLBF for individual subsystems $W_j(x_j)$, where x_j are the states of the subsystem j. We can characterize the region ϕ_{uc_j} for each subsystem j, which includes the set for which under a set of constrained control laws $u_j = \Phi_j(x) \in U_j$, the CLBF satisfies $\dot{W}_j(x_j, \Phi_j(x_j)) < -\alpha_{W_j} |W_j(x_j) - W_j(0)|$. However, in the context of DMPC where multiple controllers work collaboratively to achieve a collective control objective of guaranteeing safety and stability for each subsystem, some initial conditions may result in trajectories where the control objective for each controller in the DMPC network may lead to a conflict. For example, one controller may encounter an unsafe region for its respective local subsystem and attempts to navigate the closed-loop states away from the unsafe region, consequently increasing the Lyapunov function $V(x)$ for the overall system. On the other hand, another controller may be attempting to navigate the process state of the other subsystem to the origin, thereby decreasing $V(x)$ for the overall system. Therefore, the set of initial conditions for which the conditions of

Eq. (5) are satisfied will only be a subset of the combination of sets for which the CLBF conditions on $W_j(x_j)$ are satisfied for each subsystem individually. In other words, if the stability and safety region for each subsystem j is defined with respect to $W_j(x_j)$ as $\mathcal{U}_{\rho_j}$, $j = 1, 2$, then $\mathcal{U}_\rho \subseteq (\mathcal{U}_{\rho_1} \cup \mathcal{U}_{\rho_2})$.

An example of such CLBF-based controllers $\Phi_1(x) \in U_1 \subset \mathbf{R}^{m_1}$ and $\Phi_2(x) \in U_2 \subset \mathbf{R}^{m_2}$, is given as follows:

$$\phi_{j_i}(x) = \begin{cases} -\dfrac{p + \sqrt{p^2 + q^4}}{q^T q} q & \text{if} \quad q \neq 0 \\ 0 & \text{if} \quad q = 0 \end{cases} \tag{7a}$$

$$\Phi_{j_i}(x) = \begin{cases} u_{j_i}^{\min} & \text{if} \quad \phi_{j_i}(x) < u_{j_i}^{\min} \\ \phi_{j_i}(x) & \text{if} \quad u_{j_i}^{\min} \leq \phi_{j_i}(x) \leq u_{j_i}^{\max} \\ u_{j_i}^{\max} & \text{if} \quad \phi_{j_i}(x) > u_{j_i}^{\max} \end{cases} \tag{7b}$$

where $j = 1, 2$ represents the two candidate controllers for the two subsystems, p denotes $L_f W(x)$ where $f = [f_1 \dots f_n]^T$, and q denotes $L_{g_{j_i}} W(x)$, where $g_{j_i} = [g_{j_{i1}}, \dots, g_{j_{in}}]^T$, $(i = 1, 2, \dots, m_1$ for $j = 1$ corresponding to $\Phi_1(x)$, and $i = 1, 2, \dots, m_2$ for $j = 2$ corresponding to $\Phi_2(x)$.) $\phi_{j_i}(x)$ of Eq. (7a) denotes the i_{th} component of the control action $\phi_j(x)$. After accounting for the input constraints $u_j \in U_j$, $\Phi_{j_i}(x)$ of Eq. (7) represents the i_{th} component of the saturated control law $\Phi_j(x)$.

3.1. Design of constrained CLBF

The set $\mathcal{U}_\rho$, as defined in Eq. (4c), is a forward invariant set of $W(x)$, and it will define the set of initial conditions we consider in the rest of the manuscript. We analyze the scenario of bounded unsafe sets first following similar logic as presented in Theorem 1 in Wu and Christofides (2019), and present theoretical analysis on the closed-loop stability and safety for the nonlinear system of Eq. (1). Specifically in the case of bounded unsafe regions, stationary points in addition to the origin $x_e \in \mathcal{X}_e$ are present in state-space which can be considered as saddle points. The continuous control actions $u_1 = \Phi_1(x) \in U_1$, $u_2 = \Phi_2(x) \in U_2$ are not able to help the states escape the stationary points once the states reach them. Therefore, discontinuous control actions $u_1 = \bar{u}_1(x) \in U_1$, $u_2 = \bar{u}_2(x) \in U_2$ that decrease $W(x)$ are designed, where $[\bar{u}_1(x), \bar{u}_2(x)] \neq [\Phi_1(x), \Phi_2(x)]$, to navigate x away from these stationary points along the direction of $W(x)$ decreasing. On the other hand, in the presence of unbounded unsafe sets, the only unique stationary point in state-space is the origin, therefore $u_1 = \Phi_1(x) \in U_1$, $u_2 = \Phi_2(x) \in U_2$ are able to render the origin asymptotically stable and simultaneously guaranteeing process safety. More work on handling bounded and unbounded unsafe sets are detailed in Wu and Christofides (2019) for further reference.

4. CLBF-based control law

4.1. Effect of bounded disturbance and sample-and-hold implementation of control actions

As the CLBF will be used in the design of DMPC, which implements its control actions in a sample-and-hold manner, we need to consider the impact of sample-and-hold control as well as the presence of disturbances in the nonlinear system of Eq. (1) which are sufficiently small and bounded when analyzing stability and safety properties of the closed-loop system. We provide proof for these considerations in the next proposition.

Proposition 1. *Consider the nominal system of Eq. (1) with $w(t) \equiv 0$ and a constrained CLBF $W(x)$ that meets the requirements of Definition 3 and has a minimum at the origin. Subsequently, we characterize the set of initial conditions $\mathcal{U}_\rho \subset \mathcal{X}_0$. Let $u_1(t) = \Phi_1(x(t_k)) \in U_1$, $u_2(t) = \Phi_2(x(t_k)) \in U_2$ for all $t_k \leq t < t_{k+1}$, $x(t_k) \in \mathcal{U}_\rho \backslash \mathcal{B}_\delta(x_e)$ where $\delta > 0$, $x_e \in \mathcal{X}_e$ and t_k represents the time stamp $t = k\Delta$, $k = 0, 1, 2, \dots$, and $u_1(t) = \bar{u}_1(x) \in U_1$, $u_2(t) = \bar{u}_2(x) \in U_2$ such that if $x(t_k) \in \mathcal{B}_\delta(x_e)$, then $W(x(t_{k+1})) < W(x(t_k))$ for any $\Delta > 0$. Then, there exists a real valued Δ^*, such that, if $\Delta \in (0, \Delta^*]$ and $x_0 \in \mathcal{U}_\rho$, then $x(t) \in \mathcal{U}_\rho$, and $\lim_{t \to \infty} |x(t)| \leq d$, for any positive real number d.*

Proof. For any initial conditions in $\mathcal{U}_\rho$, we will first show that $x(t)$ converges to a terminal level set around the origin $\mathcal{U}_{\rho_{\min}} := \{x \in \phi_{uc} \mid W(x) \leq \rho_{\min}\}$ as $t \to \infty$ where $\rho_{\min} < \rho$. Then by the continuity of $W(x)$, we prove that $\lim_{t \to \infty} |x(t)| \leq d$ as $t \to \infty$. First, we consider the case when $x(t_k) \in \mathcal{U}_\rho \backslash (\mathcal{U}_{\rho_s} \cup \mathcal{B}_\delta(x_e))$, where $\rho_s < \rho_{\min} < \rho$, and demonstrate that $\dot{W}(x(t), u_1(t), u_2(t)) < -\epsilon$ holds in the set $\mathcal{Z} := \{x \in \phi_{uc} \backslash \mathcal{B}_\delta(x_e) \mid \rho_s \leq W(x) \leq \rho\}$ under $u_1(t) = u_1(t_k) = \Phi_1(x(t_k))$, $u_2(t) = u_2(t_k) = \Phi_2(x(t_k))$, $\forall\ t \in [t_k, t_k + \Delta^*)$. The time derivative of the CLBF can be represented as follows:

$$\begin{aligned} &\dot{W}(x(t), u_1(t), u_2(t)) \\ &= \dot{W}(x(t_k), u_1(t_k), u_2(t_k)) + (\dot{W}(x(t), u_1(t), u_2(t)) \\ &\quad - \dot{W}(x(t_k), u_1(t_k), u_2(t_k)) \\ &= L_f W(x(t_k)) + L_{g_1} W(x(t_k)) u_1(t_k) + L_{g_2} W(x(t_k)) u_2(t_k) \\ &\quad + (L_f W(x(t)) - L_f W(x(t_k))) \\ &\quad + (L_{g_1} W(x(t)) - L_{g_1} W(x(t_k))) u_1(t) \\ &\quad + (L_{g_2} W(x(t)) - L_{g_2} W(x(t_k))) u_2(t) \end{aligned} \tag{8}$$

□

Since $W(x)$ is a $\mathcal{C}^1$ function that satisfies Eq. (4), and $f(\cdot)$, $g_1(\cdot)$ and $g_2(\cdot)$ are assumed to be smooth, there exist positive real numbers k_f, k_{g_1} and k_{g_2}, such that $|(L_f W(x(t)) - L_f W(x(t_k))| \leq k_f |x(t) - x(t_k)|$, $|(L_{g_1} W(x(t)) - L_{g_1} W(x(t_k)))u_1(t))| \leq k_{g_1} |x(t) - x(t_k)|$, $|(L_{g_2} W(x(t)) - L_{g_2} W(x(t_k)))u_2(t))| \leq k_{g_2} |x(t) - x(t_k)|$. In addition, since $f(x)$, $g_1(x)$ and $g_2(x)$ are continuous, and $\mathcal{Z}$ is bounded, there exists a positive real number k_s and a sampling period Δ' such that $|x(t) - x(t_k)| \leq k_s \Delta'$ for all $t \in [t_k, t_k + \Delta')$. According to how ϕ_{uc} is defined, it is given that $\dot{W}(x(t_k)) < -\alpha_W |W(x) - W(0)| < -\alpha_W \rho_m$ holds for all $x \in \mathcal{Z}$, where $\rho_m := \min_{x \in \mathcal{Z}} |W(x) - W(0)|$. We choose $\Delta' < \frac{\alpha_W \rho_m - \epsilon}{k_s (k_f + k_{g_1} + k_{g_2})}$ and $0 \leq \epsilon < \alpha_W \rho_m$, where α_W is used to characterize ϕ_{uc}. Using these inequalities derived from Lipschitz conditions, Eq. (8) can be written as:

$$\begin{aligned} \dot{W}(x(t), u_1(t), u_2(t)) &\leq \dot{W}(x(t_k), u_1(t_k), u_2(t_k)) \\ &\quad + k_s (k_f + k_{g_1} + k_{g_2}) \Delta' \\ &< -\alpha_W \rho_m + k_s (k_f + k_{g_1} + k_{g_2}) \Delta' \\ &< -\epsilon \end{aligned} \tag{9}$$

which implies that for any initial conditions in $\mathcal{U}_\rho$, $W(x(t)) < W(x(t_k)) \leq \rho$, $\forall\ t > t_k$ and the closed-loop state $x(t)$ will enter a terminal set $\mathcal{U}_{\rho_s}$ within finite steps. We have proven that $x(t)$ is bounded in $\mathcal{U}_\rho$ $\forall t \in [t_k, t_k + \Delta')$.

In addition, we discuss the case where the closed-loop state is in the neighborhood of saddle points, $x(t_k) \in \mathcal{B}_\delta(x_e)$ where x_e are saddle points. Since $\bar{u}_1(x), \bar{u}_2(x)$ are a set of control actions that decrease $W(x)$, as a result, $W(x(t_{k+1})) < W(x(t_k))$ as $x(t_{k+1})$ moves to a smaller level set of $W(x)$ and the closed-loop state eventually leaves $\mathcal{B}_\delta(x_e)$ within finite time steps. After it leaves the saddle point neighborhood, $x(t)$ will not come back to $\mathcal{B}_\delta(x_e)$ as Eq. (9) (i.e., $W(x(t)) < W(x(t_k))$, $\forall\ t > t_k$) holds thereafter.

We will now address the effect of sample-and-hold control and bounded disturbance on the convergence and boundedness of the closed-loop state. First, we will show that given $x(t_k) \in \mathcal{U}_{\rho_s}$, the trajectory of $x(t)$ will stay in $\mathcal{U}_{\rho'_{\min}}$, $\forall\ t \in [t_k, t_k + \Delta'')$. Consider Δ'' such that

$$\rho'_{min} = \max_{\Delta \in [0, \Delta'')} \{W(x(t_k + \Delta)) \mid x(t_k) \in \mathcal{U}_{\rho_s},\ u \in U\}. \tag{10}$$

There exists a sufficiently small Δ'' such that Eq. (10) holds. Therefore, let $\Delta^* = \min\{\Delta', \Delta''\}$, and we have shown that for any $x(t_k) \in \mathcal{U}_{\rho_s}$, the closed-loop state $x(t)$ under sample-and-hold control implementation will remain in $\mathcal{U}_{\rho'_{\min}}$ during one sampling period $\Delta \in (0, \Delta^*]$. When taking the bounded disturbance $|w(t)| \leq w_m$ into account and the CLBF-based controller applied in a sample-and-hold fashion, we can show that Proposition 1 still holds for the system of Eq. (1) subject to the bounded disturbance. Given the local Lipschitz property of $v(\cdot)$, we can derive the following inequality for $L_v W(x)$: $\exists\ k_d > 0$, s.t. $|(L_v W(x(t)) - L_v W(x(t_k))| \leq k_d |x(t) - x(t_k)|$. Therefore, similar results can be shown for $\dot{W}(x(t), u_1(t), u_2(t))$ and $\rho_{\min}$ that account for $w(t)$ as follows:

$$\begin{aligned} &\dot{W}(x(t), \quad u_1(t), u_2(t)) \\ &\leq \dot{W}(x(t_k), u_1(t_k), u_2(t_k)) + k_s(k_f + k_{g_1} + k_{g_2} + k_d w_m)\Delta' \\ &< -\alpha_W \rho_m + k_s(k_f + k_{g_1} + k_{g_2} + k_d w_m)\Delta' \\ &< -\epsilon \end{aligned} \tag{11}$$

$$\begin{aligned} \rho_{\min} = \max_{\Delta \in [0, \Delta'')} \{ & W(x(t_k + \Delta), u_1, u_2, w) \mid x(t_k) \in \mathcal{U}_{\rho_s}, \\ & u \in U, \ |w| \leq w_m \}. \end{aligned} \tag{12}$$

where $\Delta' < \frac{\alpha_W \rho_m - \epsilon}{k_s(k_f + k_{g_1} + k_{g_2} + k_d w_m)}$ and $0 \leq \epsilon < \alpha_W \rho_m$, respectively. Hence, when sufficiently small bounded disturbance $|w| \leq w_m$ is present, $\dot{W} < 0$ still holds within each sampling period if Δ' and ϵ are chosen. Furthermore, if $x(t_k) \in \mathcal{B}_\delta(x_e)$, the discontinuous control laws $\bar{u}_1(x), \bar{u}_2(x)$ are assumed to exist and satisfy $W(x(t_{k+1})) < W(x(t_k))$, $\forall\ |w| \leq w_m$. By the definition of $\rho_{\min}$ of Eq. (12), it is shown that for any $x(t_k) \in \mathcal{U}_{\rho_s}$, the trajectory of $x(t)$ will stay in $\mathcal{U}_{\rho_{\min}}, \forall\ t \in [t_k, t_k + \Delta'')$. The proof above shows the robustness of the CLBF-based control law against the sample-and-hold execution in the presence of sufficiently small bounded disturbances, and serves as an underlying foundation for proving that the CLBF-DMPC is also robust to sample-and-hold control execution and bounded disturbances.

5. CLBF-DMPC formulations and analysis

DMPC has proven to provide improved computational time and closed-loop control performance, where some level of communication may be established between the different controllers. In this framework, two separate MPCs are designed to compute control actions u_1 and u_2 respectively; the control law trajectories computed by MPC-1 and MPC-2 are denoted by u_{d_1} and u_{d_2}, respectively. In the following few sections, we will discuss a sequential distributed MPC design and an iterative distributed MPC design; interested readers may refer to Christofides et al. (2013); Chen et al. (2021a) for other distributed and decentralised MPC architectures.

5.1. Sequential distributed MPC system

Between two MPCs in a sequential DMPC structure, the communication is one-way. In other words, the set of the optimal control laws calculated by one MPC will be relayed to the other MPC, which will utilize this additional knowledge to optimize its corresponding set of control laws. In a sequential DMPC framework, the following implementation strategy is used:

1. At each sampling instant $t = t_k$, sensor measurements on the states $x(t),\ t = t_k$ are sent to both MPC-1 and MPC-2.
2. The optimal trajectory of u_{d_1} is calculated by MPC-1 and sent to MPC-2, and the first value of the input trajectory $u^*_{d_1}(t_k)$ is sent to the corresponding actuators.
3. MPC-2 calculates the optimal trajectory of u_{d_2} based on state measurement $x(t)$ at $t = t_k$ and the optimal trajectory of u_{d_1} received from MPC-1, then sends the first optimal control action over the next sampling period $u^*_{d_2}(t_k)$ to the corresponding control actuators.
4. At the next sampling instance, when an updated state measurement is available ($k \leftarrow k+1$), go to Step 1.

In the calculation of MPC-1, it first assumes a trajectory for u_{d_2} along the prediction horizon, which is computed using the explicit nonlinear CLBF-based control law, $\Phi_2(x)$. In addition, we incorporate a contractive constraint in the optimization problem of the MPC in order to ensure that u_{d_1} will inherit the stability and safety properties of $\Phi_j(x),\ j = 1, 2$, and decrease the CLBF $W(x)$ at a minimum rate of that of the CLBF-based control laws $\Phi_j(x),\ j = 1, 2$. The optimization problem of MPC-1 is given as follows:

$$\mathcal{J} = \min_{u_{d_1} \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), u_{d_1}(t), \Phi_2(\tilde{x}(t)))dt \tag{13a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u_{d_1}(t), \Phi_2(\tilde{x}(t))) \tag{13b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{13c}$$

$$u_{d_1}(t) \in U_1, \ \forall\ t \in [t_k, t_{k+N}) \tag{13d}$$

$$\dot{W}\big(x(t_k), u_{d_1}(t_k), \Phi_2(x(t_k))\big) \leq \dot{W}(x(t_k), \Phi_1(x(t_k)), \Phi_2(x(t_k))), \tag{13e}$$

$$\text{if } x(t_k) \notin \mathcal{B}_\delta(x_e) \text{ and } W(x(t_k)) > \rho_s \tag{13f}$$

$$W(\tilde{x}(t)) \leq \rho_s, \ \forall\ t \in [t_k, t_{k+N}), \ \text{if } W(x(t_k)) \leq \rho_s \tag{13g}$$

$$W(\tilde{x}(t)) < W(x(t_k)), \ \forall\ t \in (t_k, t_{k+N}), \quad \text{if } x(t_k) \in \mathcal{B}_\delta(x_e) \tag{13h}$$

where $S(\Delta)$ is the set of piece-wise constant functions with sampling period Δ, N is the number of sampling periods in the prediction horizon, and $\tilde{x}$ represents the predicted state trajectory. The optimal input trajectory calculated over the prediction horizon $t \in [t_k, t_{k+N})$ by MPC-1 is denoted as $u^*_{d_1}(t)$. The cost function of Eq. (13a) is the integral of $L(\tilde{x}(t), u_{d_1}(t), \Phi_2(t))$ over the prediction horizon; here, $L(x, u_1, u_2)$ typically takes on a quadratic form, i.e., $L(x, u_1, u_2) = x^T Q x + u_1^T R_1 u_1 + u_2^T R_2 u_2$, where Q, R_1, and R_2 are positive definite weighting matrices. The minimum value of the objective function of Eq. (13a) is at the origin. The constraint of Eq. (13b) is the nominal system of Eq. (1) with $w(t) \equiv 0$ and predicts the closed-loop state trajectory. Eq. (13d) defines the input variable constraints on u_{d_1}. The initial condition $\tilde{x}(t_k)$ of Eq. (13b) is taken as the state sensor measurement at $t = t_k$ defined in Eq. (13c). The constraints of Eqs. (13f)–(13h) are activated depending on the location of the process state in state-space, and they work together to make certain of operational safety and stability. When $x(t_k) \notin \mathcal{B}_\delta(x_e)$ and $W(x(t_k)) > \rho_s$, the constraint Eq. (13f) ensures that $W(\tilde{x})$ decreases at least as fast as the rate achieved by the CLBF-based control laws $u_1 = \Phi_1(x) \in U_1,\ u_2 = \Phi_2(x) \in U_2$. If $W(x(t_k)) \leq \rho_s$, the constraint of Eq. (13g) maintains the predicted state within $\mathcal{U}_{\rho_s}$, so that in the presence of sufficiently bounded disturbances in the nonlinear system of Eq. (1), the closed-loop state still remains in $\mathcal{U}_{\rho_{\min}}$. Furthermore, if $x(t_k)$ enters a neighborhood of a saddle point $\mathcal{B}_\delta(x_e)$, the constraint Eq. (13h) ensures that $W(x)$ decreases over the predicted trajectory, and with decreasing $W(x)$, the closed-loop process state can eventually escape x_e within finite steps. Once the state escapes from the saddle points $\mathcal{B}_\delta(x_e)$, the constraint of Eq. (13f) will drive

it towards the origin into smaller level sets of the CLBF $W(x)$, thus guaranteeing the state will not return to $\mathcal{B}_\delta(x_e)$ thereafter. Each time MPC-1 is executed, it communicates the entire trajectory of $u^*_{d_1}(t),\ t \in [t_k, t_{k+N})$ to MPC-2 and sends the first value of the input trajectory $u^*_{d_1}(t_k)$ to its actuators. The horizon rolls one sampling time step forward while the above optimization problem is solved again.

MPC-2 computes control actions u_{d_2} based on the latest received state measurement, and in addition, the control action computed by MPC-1 (i.e., $u^*_{d_1}(t), \forall t \in [t_k, t_{k+N})$). By utilizing the optimal input trajectory of MPC-1 as well as the CLBF-based control law $\Phi_2(x(t_k))$, the closed-loop performance is optimized while guaranteeing that the stability and safety properties of the CLBF-based control laws are preserved. Specifically, MPC-2 calculates the following optimization problem:

$$\mathcal{J} = \min_{u_{d_2} \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), u^*_{d_1}(t), u_{d_2}(t))dt \tag{14a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u^*_{d_1}(t), u_{d_2}(t)) \tag{14b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{14c}$$

$$u_{d_2}(t) \in U_2,\ \forall\ t \in [t_k, t_{k+N}) \tag{14d}$$

$$\dot{W}\left(x(t_k), u^*_{d_1}(t_k), u_{d_2}(t_k)\right) \le \dot{W}\left(x(t_k), u^*_{d_1}(t_k), \Phi_2(x(t_k))\right), \tag{14e}$$

$$\text{if } x(t_k) \notin \mathcal{B}_\delta(x_e) \text{ and } W(x(t_k)) > \rho_s \tag{14f}$$

$$W(\tilde{x}(t)) \le \rho_s,\ \forall\ t \in [t_k, t_{k+N}),\ \text{if } W(x(t_k)) \le \rho_s \tag{14g}$$

$$W(\tilde{x}(t)) < W(x(t_k)),\ \forall\ t \in (t_k, t_{k+N}),$$
$$\text{if } x(t_k) \in \mathcal{B}_\delta(x_e) \tag{14h}$$

The notation and the explanation of the optimization problem of MPC-2 are akin to that of MPC-1 and will be omitted here for brevity. To account for the total computation time for the sequential DMPC framework, one would add the times taken to solve each MPC problem respectively, since the solution of MPC-2 depends on the MPC-1 results.

5.2. Iterative distributed MPC system

The communication between two MPCs in an iterative framework is two-ways. The optimal control actions calculated by each MPC are exchanged to better predict future states, and the optimization problem in each MPC is solved independently in a parallel structure until an iteration criterion has been met. The implementation strategy is as follows:

1. MPC-1 and MPC-2 receive the state sensor measurement $x(t)$ at $t = t_k$ at each sampling instant t_k.
2. At iteration $c = 1$, MPC-1 calculates $u_{d_1}(t)$ over the prediction horizon assuming $u_2(t) = \Phi_2(t), \forall t \in [t_k, t_{k+N})$. MPC-2 calculates $u_{d_2}(t)$ over the prediction horizon assuming $u_1(t) = \Phi_1(t), \forall t \in [t_k, t_{k+N})$. The future trajectories of $u_{d_1}(t)$ and $u_{d_2}(t)$ are exchanged between the two MPCs, and each MPC calculates and stores the value of its own cost function.
3. At iteration $c > 1$:
   (a) Based on state measurement $x(t_k)$ as well as the latest input trajectories received from the other MPC, each MPC evaluates its own future input trajectory again.
   (b) The MPCs cross-communicate their newest calculated future input trajectories. Each MPC computes then stores the value of its cost function.
4. If a termination criterion is met, each MPC selects the input trajectory corresponding to the smallest cost function value, and sends the first control action of this optimal trajectory to its actuators. If the termination criterion is not satisfied, go to Step 3 ($c \leftarrow c + 1$).
5. At the next sampling instance, when an updated state measurement is available, go to Step 1 ($k \leftarrow k + 1$).

The optimization problem of MPC-1 in an iterative distributed LMPC at iteration $c = 1$ is presented as follows. Readers may refer to the formulations of sequential DMPC design for detailed definitions of the same variables and constraints.

$$\mathcal{J} = \min_{u_{d_1} \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), u_{d_1}(t), \Phi_2(\tilde{x}(t)))dt \tag{15a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u_{d_1}(t), \Phi_2(\tilde{x}(t))) \tag{15b}$$

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

$$u_{d_1}(t) \in U_1,\ \forall\ t \in [t_k, t_{k+N}) \tag{15d}$$

$$\dot{W}\left(x(t_k), u_{d_1}(t_k), \Phi_2(x(t_k))\right) \le \dot{W}(x(t_k), \Phi_1(x(t_k)), \Phi_2(x(t_k))), \tag{15e}$$

$$\text{if } x(t_k) \notin \mathcal{B}_\delta(x_e) \text{ and } W(x(t_k)) > \rho_s \tag{15f}$$

$$W(\tilde{x}(t)) \le \rho_s,\ \forall\ t \in [t_k, t_{k+N}),\ \text{if } W(x(t_k)) \le \rho_s \tag{15g}$$

$$W(\tilde{x}(t)) < W(x(t_k)),\ \forall\ t \in (t_k, t_{k+N}),$$
$$\text{if } x(t_k) \in \mathcal{B}_\delta(x_e) \tag{15h}$$

At iteration $c = 1$, the optimization problem of MPC-2 is shown as follows:

$$\mathcal{J} = \min_{u_{d_2} \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), \Phi_1(\tilde{x}(t)), u_{d_2}(t))dt \tag{16a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), \Phi_1(\tilde{x}(t)), u_{d_2}(t)) \tag{16b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{16c}$$

$$u_{d_2}(t) \in U_2,\ \forall\ t \in [t_k, t_{k+N}) \tag{16d}$$

$$\dot{W}\left(x(t_k), \Phi_1(x(t_k)), u_{d_2}(t_k)\right) \le \dot{W}(x(t_k), \Phi_1(x(t_k)), \Phi_2(x(t_k))), \tag{16e}$$

$$\text{if } x(t_k) \notin \mathcal{B}_\delta(x_e) \text{ and } W(x(t_k)) > \rho_s \tag{16f}$$

$$W(\tilde{x}(t)) \le \rho_s,\ \forall\ t \in [t_k, t_{k+N}),\ \text{if } W(x(t_k)) \le \rho_s \tag{16g}$$

$$W(\tilde{x}(t)) < W(x(t_k)),\ \forall\ t \in (t_k, t_{k+N}),$$
$$\text{if } x(t_k) \in \mathcal{B}_\delta(x_e) \tag{16h}$$

At iteration $c > 1$, after the optimized input trajectories $u^*_{d_1}(t)$ and $u^*_{d_2}(t)$ have been exchanged between the two MPCs, the optimization problem of MPC-1 becomes:

$$\mathcal{J} = \min_{u_{d_1} \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), u_{d_1}(t), u^*_{d_2}(t))dt \tag{17a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u_{d_1}(t), u^*_{d_2}(t)) \tag{17b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{17c}$$

$$u_{d_1}(t) \in U_1, \ \forall\ t \in [t_k, t_{k+N}) \tag{17d}$$

$$\dot{W}\left(x(t_k), u_{d_1}(t_k), u^*_{d_2}(t)\right) \leq \dot{W}(x(t_k), \Phi_1(x(t_k)), \Phi_2(x(t_k))), \tag{17e}$$

$$\text{if } x(t_k) \notin \mathcal{B}_\delta(x_e) \text{ and } W(x(t_k)) > \rho_s \tag{17f}$$

$$W(\tilde{x}(t)) \leq \rho_s, \ \forall\ t \in [t_k, t_{k+N}), \ \text{if } W(x(t_k)) \leq \rho_s \tag{17g}$$

$$W(\tilde{x}(t)) < W(x(t_k)), \ \forall\ t \in (t_k, t_{k+N}), \ \text{if } x(t_k) \in \mathcal{B}_\delta(x_e) \tag{17h}$$

And the optimization problem of MPC-2 becomes:

$$\mathcal{J} = \min_{u_{d_2} \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), u^*_{d_1}(t), u_{d_2}(t))dt \tag{18a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u^*_{d_1}(t), u_{d_2}(t)) \tag{18b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{18c}$$

$$u_{d_2}(t) \in U_2, \ \forall\ t \in [t_k, t_{k+N}) \tag{18d}$$

$$\dot{W}\left(x(t_k), u^*_{d_1}(t_k), u_{d_2}(t)\right) \leq \dot{W}(x(t_k), \Phi_1(x(t_k)), \Phi_2(x(t_k))), \tag{18e}$$

$$\text{if } x(t_k) \notin \mathcal{B}_\delta(x_e) \text{ and } W(x(t_k)) > \rho_s \tag{18f}$$

$$W(\tilde{x}(t)) \leq \rho_s, \ \forall\ t \in [t_k, t_{k+N}), \ \text{if } W(x(t_k)) \leq \rho_s \tag{18g}$$

$$W(\tilde{x}(t)) < W(x(t_k)), \ \forall\ t \in (t_k, t_{k+N}), \ \text{if } x(t_k) \in \mathcal{B}_\delta(x_e) \tag{18h}$$

Since the two MPCs in an iterative framework can be simultaneously solved in a parallel structure using separate processors, the total computation time would equal to the maximum time of the two MPCs including all iterations taken until termination of iterations. The total number of iterations would depend on the termination criterion. Some examples of these criteria may include, the total iterations must not exceed a maximum threshold, $c \leq c_{\max}$; the computation time each MPC takes must not surpass a time threshold; between two consecutive iterations, the difference in the cost function value or the computed trajectory of control actions must be sufficiently small.

Remark 2. In this work, we have presented the formulations and simulations of DMPC systems in the case of two subsystems (and thus, two controllers) for simplicity of notation, but the results are conceptually straightforward and can be similarly extended to the case of N_{sys} subsystems having N_{sys} controllers in total.

Once solving both optimization problems of MPC-1 and MPC-2 is complete, the proposed CLBF-DMPC provides the optimal control actions in the following form:

$$\begin{aligned} u_1(t) &= u^*_{d_1}(t_k), \forall t \in [t_k, t_{k+1}) \\ u_2(t) &= u^*_{d_2}(t_k), \forall t \in [t_k, t_{k+1}) \end{aligned} \tag{19}$$

The control actions computed by each MPC will be applied in a sample-and-hold manner to the nonlinear process of Eq. (1) with bounded disturbances.

We will now demonstrate that, for the nonlinear system of Eq. (1), stability and safety can be established under the CLBF-based DMPC system with the theorem and proof below. Note that the proof is written with respect to the sequential DMPC, but the same concept can be applied to the iterative DMPC as well.

Theorem 1. *Consider the system described by Eq. (1), and it has a constrained CLBF $W(x)$ that satisfies Eq. (4) with its minimum value at the origin. Given any initial condition $x_0 \in \mathcal{U}_\rho$, the CLBF-DMPC optimization problems of Eqs. (13) and (14) are guaranteed to have recursive feasibility for all times, and under the sample-and-hold implementation of CLBF-DMPC control actions $[u_1 \ \ u_2] = [u^*_{d_1} \ \ u^*_{d_2}]$, $x(t)$ is bounded in $\mathcal{U}_\rho$ for all $t \geq 0$, and as $t \to \infty$, converges to $\mathcal{U}_{\rho_{\min}}$.*

Proof.

Part 1: In Eq. (13) and (14), the optimization problems of the CLBF-DMPC have feasible solutions at all times, and this is because the CLBF-DMPC constraints of Eqs. (13d), (13h), and (14d), (14h) can be met respectively by the sample-and-hold implementation of control actions $u_1 = \bar{u}_1(x) \in U_1, \ u_2 = \bar{u}_2(x) \in U_2, \ \forall x \in \mathcal{B}_\delta(x_e)$ and $u_1 = \Phi_1(x) \in U_1, \ u_2 = \Phi_2(x) \in U_2, \ \forall x \in \mathcal{U}_\rho \backslash \mathcal{B}_\delta(x_e)$. By letting $u_1(t_k) = \Phi_1(x(t_k)), \ u_2(t_k) = \Phi_2(x(t_k))$ when $x(t_k) \in \mathcal{U}_\rho \backslash (\mathcal{B}_\delta(x_e) \cup \mathcal{U}_\rho)$, Eqs. (13f) and (14f) are also satisfied. In Proposition 1, we have shown that once x is driven inside $\mathcal{U}_{\rho_s}$ by the CLBF-based control laws $u_1 = \Phi_1(x) \in U_1, \ u_2 = \Phi_2(x) \in U_2$, it will not exit $\mathcal{U}_{\rho_{\min}}$ within one sampling period for any $u_1 \in U_1, \ u_2 \in U_2$. Therefore, the CLBF-based control laws are able to provide a feasible solution for the input trajectories and satisfy the constraints of Eqs. (13g) and (14g). Lastly, as the controller $u_1 = \bar{u}_1(x) \in U_1, \ u_2 = \bar{u}_2(x) \in U_2$ are able to satisfy $W(x(t_{k+1})) < W(x(t_k))$, the control action $u_j(t) = \bar{u}_j(x(t_{k+i})) \in U_j$, for $j = 1, 2, \ \forall\ t \in [t_{k+i}, t_{k+i+1})$ with $i = 0, \ldots, N-1$ will satisfy the constraints of Eqs. (13h) and (14h) and eventually navigate the states away from the stationary saddle points if $x(t_k) \in \mathcal{B}_\delta(x_e)$.

Part 2: We will now demonstrate simultaneous stability and safety for the nonlinear system of Eq. (1) can be guaranteed under the optimized solutions of Eqs. (13) and (14). For any $x_0 \in \mathcal{U}_\rho \backslash \mathcal{U}_{\rho_s}$, the constraints of Eqs. (13f) and (14f) ensure that the CLBF-DMPC control actions $u^*_{d_1}$, and sequentially $u^*_{d_2}$, are optimized to decrease the value of the CLBF and will drive x towards the origin; the closed-loop state x will eventually enter $\mathcal{U}_{\rho_s}$ within finite sampling steps. □

After x enters $\mathcal{U}_{\rho_s}$, the constraints of Eqs. (13g) and (14g) ensure the boundedness of the closed-loop state in $\mathcal{U}_{\rho_{\min}}$ for the remaining time considering the impact of sample-and-hold control and the presence of bounded disturbance. As the safe operating region $\mathcal{U}_\rho$ does not intersect with the unsafe region $\mathcal{D}$, x will not enter $\mathcal{D}$ for all times and will remain inside $\mathcal{U}_\rho$ for any $x_0 \in \mathcal{U}_\rho$. With $x_0 \in \mathcal{U}_\rho \backslash \mathcal{U}_{\rho_s}$, the constraints of Eqs. (13f) and (14f) pull the state towards the origin. The constraint of Eqs. (13h) and (14h) will be activated when x arrives at a saddle point neighborhood, i.e.,

$x(t_k) \in \mathcal{B}_\delta(x_e)$; x will be driven away from $\mathcal{B}_\delta(x_e)$ in the direction of $W(x)$ decreasing. After it leaves from $\mathcal{B}_\delta(x_e)$, the DMPC constraints of Eqs. (13f), (13g) and (14f), (14g) will take over and continue to ensure closed-loop safety and stability thereafter; ultimately, the closed-loop state converges towards the origin and is bounded in $\mathcal{U}_{\rho_{\min}}$. Thus, closed-loop stability and safety under the sample-and-hold implementation of CLBF-DMPC for the nonlinear system of Eq. (1) with sufficiently bounded disturbance in the presence of bounded unsafe sets have been shown.

5.3. Modified DMPC structure in special cases

In many industrial processes, there are examples where the process variables of an upstream sub-process impact the dynamics of a downstream sub-process, but not vice versa. In these cases where the first subsystem is independent and the second subsystem is dependent on the first subsystem, we can design the DMPC with some special considerations to assess whether safety and stability can be simultaneously guaranteed. We use sequential DMPC as an example. Since the first subsystem is completely independent, its contractive constraint of Eq. (13f) can be modified to only account for the CLBF of subsystem-1 $\dot{W}_j,\ j=1$, and therefore only depends on the states and inputs of subsystem-1, $x_j(t_k),\ u_j$ where $j=1$. In doing so, MPC-1 can guarantee the stability and safety of the upstream process, subsystem-1. The contractive constraint of Eq. (14f) can also be similarly modified to account for the CLBF function of subsystem-2 only, $\dot{W}_j,\ j=2$, where $\dot{W}_2(x_1, x_2, u_2)$ can be simplified to be a function of x_1 of subsystem-1, x_2 of subsystem-2, and u_2 of subsystem-2. This leads to a modified formulation of the DMPC system with simpler computation complexity. However, since the constraints to each controller are only with respect to its own subsystem, one caveat to this modification is that the state measurements of subsystem-1 will be treated as disturbances in the computation of MPC-2. Therefore, as we will demonstrate with a nonlinear example in Section 6, there are values of states for subsystem-1 that may result in non-negative values of $\dot{W}_2$ for subsystem-2.

The DMPC formulation for such processes can be modified for improved computation time and algorithm simplicity. Using sequential DMPC as an example, the optimization problem of MPC-1 is as follows:

$$\mathcal{J} = \min_{u_{d_1}\in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), u_{d_1}(t), \Phi_2(\tilde{x}(t)))dt \tag{20a}$$

$$\text{s.t.}\quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u_{d_1}(t), \Phi_2(\tilde{x}(t))) \tag{20b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{20c}$$

$$u_{d_1}(t) \in U_1,\ \forall\ t \in [t_k, t_{k+N}) \tag{20d}$$

$$\dot{W}_1\big(x_1(t_k), u_{d_1}(t_k)\big) \le \dot{W}_1(x_1(t_k), \Phi_1(x(t_k))), \tag{20e}$$

$$\text{if } x_1(t_k) \notin \mathcal{B}_{\delta_1}(x_{1e}) \text{ and } W_1(x_1(t_k)) > \rho_{s_1} \tag{20f}$$

$$W_1(\tilde{x}_1(t)) \le \rho_{s_1},\ \forall\ t \in [t_k, t_{k+N}),\ \text{if } W_1(x_1(t_k)) \le \rho_{s_1} \tag{20g}$$

$$W_1(\tilde{x}_1(t)) < W_1(x_1(t_k)),\ \forall\ t \in (t_k, t_{k+N}),\ \text{if } x_1(t_k) \in \mathcal{B}_{\delta_1}(x_{1e}) \tag{20h}$$

where the level sets of $W_j(x_j)$ will be respectively defined with positive real constants $\rho_{s_j},\ j=1,2$, and the neighborhood of saddle points present in the stability and safety region of the subsystem-j will be correspondingly denoted as $\mathcal{B}_{\delta_j}(x_{je})$.

The predicted state trajectory calculation of subsystem-2 $\tilde{x}_2$ relies on the state measurements of subsystem-1 $x_1(t_k)$. The calculation of $\dot{W}_2$ will need the measurements of $x_1(t_k)$ in addition to $x_2(t_k)$ and $u_2(t_k)$. Note that the full state vector is the combination of states of subsystems 1 and 2, i.e., $x(t_k)^T = [x_1(t_k)^T, x_2(t_k)^T]$. Therefore, the formulation of the modified MPC-2 in a sequential distributed design is as follows:

$$\mathcal{J} = \min_{u_{d_2}\in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(t), u^*_{d_1}(t), u_{d_2}(t))dt \tag{21a}$$

$$\text{s.t.}\quad \dot{\tilde{x}}(t) = F(\tilde{x}(t), u^*_{d_1}(t), u_{d_2}(t)) \tag{21b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{21c}$$

$$u_{d_2}(t) \in U_2,\ \forall\ t \in [t_k, t_{k+N}) \tag{21d}$$

$$\dot{W}_2\big(x(t_k), u_{d_2}(t_k)\big) \le \dot{W}_2(x(t_k), \Phi_2(x(t_k))), \tag{21e}$$

$$\text{if } x_2(t_k) \notin \mathcal{B}_{\delta_2}(x_{2e}) \text{ and } W_2(x_2(t_k)) > \rho_{s_2} \tag{21f}$$

$$W_2(\tilde{x}_2(t)) \le \rho_{s_2},\ \forall\ t \in [t_k, t_{k+N}),\ \text{if } W_2(x_2(t_k)) \le \rho_{s_2} \tag{21g}$$

$$W_2(\tilde{x}_2(t)) < W_2(x_2(t_k)),\ \forall\ t \in (t_k, t_{k+N}),\ \text{if } x_2(t_k) \in \mathcal{B}_{\delta_2}(x_{2e}) \tag{21h}$$

A similar modification can be applied to iterative DMPC structures. Following the MPC-1 calculation, closed-loop stability and safety can be guaranteed for subsystem-1 using the CLBF-based constraints on W_1. Since subsystem-2 is dependent on the states of subsystem-1 and since the calculation of MPC-2 is carried out with CLBF-based constraints on W_2 only, there may exist points in state space where the explicit control law $\Phi_2(x(t_k))$ can no longer guarantee a negative $\dot{W}_2(x(t_k), \Phi_2(x(t_k)))$ given the impact from the state measurements of subsystem-1 $x_1(t_k)$. When this happens, the optimizer for MPC-2 may still attempt to find a set of input trajectory $u^*_{d_2}$ that decreases W_2, i.e., $\dot{W}_2(x(t_k), u_{d_2}(t_k)) < 0$. Alternatively, MPC-2 can opt to use the discontinuous control actions $\bar{u}_2(x) \in U_2$, which ensures the existence of a solution for $u^*_{d_2}$ that will decrease $W_2(\tilde{x}_2)$ along the predicted trajectory.

Remark 3. With respect to the use of a Barrier function to express safety specifications, it is important to note that the Barrier Function plays essentially the role of a safety constraint (i.e., temperature needs to be below a certain value or a nonlinear function of several state variables needs to be within a certain range) but it is implemented within the MPC scheme in a way that ensure that the closed-loop state does not enter the unsafe set (i.e., region of increased risk) in a guaranteed manner (simply, setting up a constraint in the MPC to require that the closed-loop state does not enter in a certain unsafe region cannot ensure that such an excursion of the closed-loop state to the unsafe set will not occur). Regions in state-space where the system trajectory may be allowed to enter, but due to increasing safety risk the state should not stay there long, can be formulated as soft constraints in MPC,

and have been studied in past works (Zhang et al., 2019). Such soft constraints can be added in the DMPC framework presented in this work as they do not lead to infeasibility of the MPC optimization problem. In the case where the closed-loop state is allowed to enter the unsafe region for a particular subsystem, the amount of time a controller takes to return the closed-loop system state to a safe region is related to the speed of the closed-loop response under the CLBF-based DMPC, which can be tuned by adjusting the weights in the MPC cost function. Finally, it is important to note that if there exist model uncertainties and process disturbances that lead to process/model mismatch, the proposed DMPC provides a robustness margin to sufficiently small bounded disturbances through the negative margin in the Lyapunov function time-derivative, which is a consequence of the use of measurement feedback in MPC at each sampling time.

6. Application to a nonlinear chemical process

We will demonstrate the proposed CLBF-DMPC method on a chemical process example, which consists of two well-mixed, non-isothermal continuous stirred tank reactors (CSTRs) in series. An irreversible second-order exothermic reaction takes place in each reactor that transforms a reactant A to a product B ($A \rightarrow B$). Each CSTR is fed with reactant material A with the inlet concentration C_{Aj0}, the inlet temperature T_{j0} and feed volumetric flow rate of the reactor F_{j0}, $j = 1, 2$, where $j = 1$ denotes the first CSTR and $j = 2$ denotes the second CSTR. The reactors are equipped with heating jackets to remove/supply heat at a rate Q_j, $j = 1, 2$. This system can be modelled by the following material and energy balance equations:

$$\frac{dC_{A1}}{dt} = \frac{F_{10}}{V_1}(C_{A10} - C_{A1}) - k_0 e^{\frac{-E}{RT_1}} C_{A1}^2 \tag{22a}$$

$$\frac{dT_1}{dt} = \frac{F_{10}}{V_1}(T_{10} - T_1) + \frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{RT_1}} C_{A1}^2 + \frac{Q_1}{\rho_L C_p V_1} \tag{22b}$$

$$\frac{dC_{B1}}{dt} = -\frac{F_{10}}{V_1} C_{B1} + k_0 e^{\frac{-E}{RT_1}} C_{A_1}^2 \tag{22c}$$

$$\frac{dC_{A2}}{dt} = \frac{F_{20}}{V_2} C_{A20} + \frac{F_{10}}{V_2} C_{A1} - \frac{F_{10} + F_{20}}{V_2} C_{A2} \tag{22d}$$

$$-k_0 e^{\frac{-E}{RT_2}} C_{A2}^2 \tag{22e}$$

$$\frac{dT_2}{dt} = \frac{F_{20}}{V_2} T_{20} + \frac{F_{10}}{V_2} T_1 - \frac{F_{10} + F_{20}}{V_2} T_2 \tag{22f}$$

$$+\frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{RT_2}} C_{A2}^2 + \frac{Q_2}{\rho_L C_p V_2} \tag{22g}$$

$$\frac{dC_{B2}}{dt} = \frac{F_{10}}{V_2} C_{B1} - \frac{F_{10} + F_{20}}{V_2} C_{B2} + k_0 e^{\frac{-E}{RT_2}} C_{A2}^2 \tag{22h}$$

where Q_j, V_j, C_{Aj}, T_j, where $j = 1, 2$, are the heat input rate, the volume of the reacting liquid, concentration of reactant A, and the temperature in the first and the second reactor, respectively. ΔH, E, k_0, and R represent the enthalpy of the reaction, activation energy, pre-exponential constant, and ideal gas constant, respectively. All process parameter values can be found in Table 1. The manipulated inputs for both CSTRs are the inlet concentration of species A and the heat input rate, which are in deviation variable representations $\Delta C_{Aj0} = C_{Aj0} - C_{Aj0_s}$, $\Delta Q_j = Q_j - Q_{j_s}$, $j = 1, 2$, respectively. The manipulated inputs have their respective lower and upper bounds: $|\Delta C_{Aj0}| \leq 3.5$ kmol/m^3 and $|\Delta Q_j| \leq 5 \times 10^5$ kJ/h, $j = 1, 2$. The states of the two-CSTR system are $x^T = [C_{A1} - C_{A1_s} \quad T_1 - T_{1_s} \quad C_{A2} - C_{A2_s} \quad T_2 - T_{2_s}]$, where C_{A1_s}, C_{A2_s}, T_{1_s} and T_{2_s} are the steady-state values of concentration of A and temperature in the two reactors, such that the operating steady-state and equilibrium of the nonlinear system is at the origin of the state-space. States of the CSTR-1 can be separately denoted as $[x_1, x_2] = [C_{A1} - C_{A1_s} \quad T_1 - T_{1_s}]$ and the states of the CSTR-2 are denoted as $[x_3, x_4] = [C_{A2} - C_{A2_s} \quad T_2 - T_{2_s}]$. In a distributed MPC framework, both MPCs have knowledge of full-state measurements as well as the overall plant model of the two-CSTR process. Feedback measurements on $x(t)$ are received by both MPCs, where MPC-1 optimizes $[u_1, u_2] = [\Delta C_{A10} \quad \Delta Q_1]$ and MPC-2 optimizes $[u_3, u_4] = [\Delta C_{A20} \quad \Delta Q_2]$. The common control objective of the two MPCs is to stabilize the two-CSTR process at the unstable operating steady-state $x_s^T = [C_{A1_s} \quad C_{A2_s} \quad T_{1_s} \quad T_{2_s}] = [1.9537 \text{ kmol/m}^3, \quad 1.9537 \text{ kmol/m}^3, \quad 401.9 \text{ K}, \quad 401.9 \text{ K}]$. To numerically simulate the dynamic ODE model of Eq. (22), we use the explicit Euler method with an integration time step of $h_c = 10^{-5}$ h. We demonstrate our simulations with the sequential DMPC framework. The nonlinear optimization problems of the sequential DMPC of Eqs. (20) and (21) are calculated every sampling period $\Delta = 10^{-3}$ h using the Python module of the IPOPT software package (Wächter and Biegler, 2006). The objective function in the DMPC optimization problem has the form $L(x, u_1, u_2) = x^T Q x + u_1^T R_1 u_1 + u_2^T R_2 u_2$, where $Q = diag[2 \times 10^3 \quad 1 \quad 2 \times 10^3 \quad 1]$, $R_1 = R_2 = diag[8 \times 10^{-13} \quad 0.001]$; the same objective function is used in both MPC-1 and MPC-2. Due to the special structure of the nonlinear process studied, where the first CSTR is completely independent of the second CSTR, we can adopt the modified DMPC design in Eqs. (20) and (21). In this manuscript, we present the simulation results of a sequential DMPC; however, the same closed-loop performance can be similarly demonstrated with an iterative DMPC.

We first consider a bounded unsafe region $\mathcal{D}_b$, which is embedded fully in the closed-loop system stability region, and is located in the middle of the stability region, as shown in Fig. 1. This is so that the state will encounter this unsafe set on its trajectory as it converges towards the origin if no safety control is considered. It is challenging to handle such unsafe sets for the CLBF-DMPC as the closed-loop state needs to be driven around the unsafe set, towards the steady-state thereafter, and ultimately bounded in a neighborhood around the steady-state. In this work, we consider an ellipsoid described as $\mathcal{D}_b := \{x \in \mathbf{R}^4 \mid h_1(x) = (x_1 + 0.92)^2 + \frac{(x_2 - 42)^2}{500} < 0.06, \; h_2(x) = (x_3 + 0.92)^2 + \frac{(x_4 - 42)^2}{500} < 0.06\}$. By following the design method in Wu and Christofides (2019), we can define the set $\mathcal{H}$ which encloses $\mathcal{D}$ as $\mathcal{H} := \{x \in \mathbf{R}^4 \mid h_1(x) \leq 0.07, h_2(x) \leq 0.07\}$. Then, the CBF $B_j(x)$, $j = 1, 2$ can be constructed as follows:

$$B_j(x) = \begin{cases} e^{\frac{h_j(x)}{h_j(x) - 0.07}} - e^{-6}, & \text{if } x \in \mathcal{H} \\ -e^{-6}, & \text{if } x \notin \mathcal{H} \end{cases} \tag{23}$$

From Eq. (23), it is guaranteed that $B(x)$ is positive in the unsafe region $\mathcal{D}$. The overall CLBF is the sum of the CLBFs for the two CSTRs, i.e., $W(x) = W_1(x) + W_2(x) = V_1(x) + V_2(x) + \mu(B_1(x) + B_2(x)) + \nu$ where $V_1(x) = x_1^T P_1 x_1$ and $V_2(x) = x_2^T P_2 x_2$. $\mathcal{U}_\rho$, which is safe operating region and the set of valid initial conditions, is defined with $\rho = 0$ as per Eq. (4c). $W(x)$ is designed using $\nu = -340$, $\mu = 1 \times 10^9$, which are selected based on the design method in (Wu and Christofides, 2019), and the following positive definite P matrices:

$$P_1 = P_2 = \begin{bmatrix} 1060 & 22 \\ 22 & 0.52 \end{bmatrix} \tag{24}$$

Table 1
Values and descriptions of process parameters and steady-states of state and input variables.

Parameter/value	Description
$F_{10}, F_{20} = 5$ m^3/h	Feed flow rate of CSTR 1 & 2
$T_{10} = 300$ K, $T_{20} = 300$ K	Feed temperatures of CSTR 1 & 2
$V_1 = 1.0$ m^3, $V_2 = 1.0$ m^3	Volume of reacting liquid in CSTR 1 & 2
$k_0 = 8.46 \times 10^6$ h^{-1}	Pre-exponential constant
$E = 5.0 \times 10^4$ kJ/kmol	Activation energy
$\Delta H = -1.15 \times 10^4$ kJ/kmol,	Enthalpy of reaction
$C_p = 0.231$ kJ/(kg K)	Heat capacity
$R = 8.314$ kJ/(kmol K)	Gas constant
$\rho = 1000$ kg/m^3	Liquid solution density
$C_{A10_s} = 4$ kmol/m^3, $C_{A20_s} = 4$ kmol/m^3	Inlet concentration steady-state values
$Q_{1_s} = 0$ kJ/hr, $Q_{2_s} = 0$ kJ/hr	Heat input rate steady-state values
$C_{A1_s} = 1.9537$ kmol/m^3, $C_{A2_s} = 1.9537$ kmol/m^3	Concentration of reactant A steady-state values
$T_{1_s} = 401.9$ K, $T_{2_s} = 401.9$ K	Temperature steady-state values

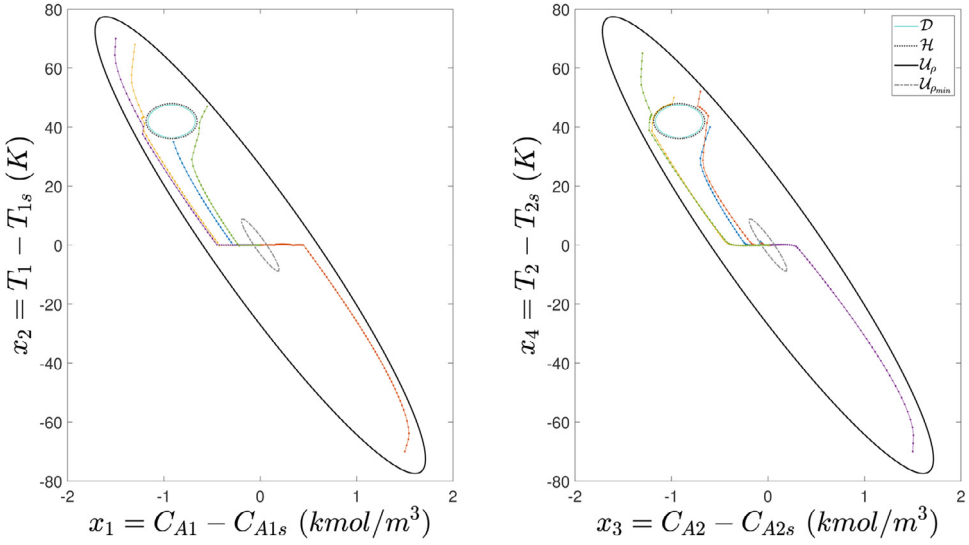

Fig. 1. Closed-loop trajectories of CSTR-1 and CSTR-2 under the sequential CLBF-DMPC in the presence of a bounded unsafe set.

Similarly, we also study the scenario of unbounded unsafe region, which is defined as $\mathcal{D}_u := \{x \in \mathbf{R}^4 \mid h_1(x) = x_1 + x_2 > 7.2,\ h_2(x) = x_3 + x_4 > 7.2\}$. The enclosing compact set $\mathcal{H}$ is defined as $\mathcal{H} := \{x \in \mathbf{R}^4 \mid h_1(x) > 6.8, h_2(x) > 6.8\}$, and the corresponding CBFs for the two subsystems $B_j(x),\ j = 1, 2$ are shown as follows:

$$B_j(x) = \begin{cases} e^{h_j(x)-7.2} - 2 \times e^{-0.4}, & \text{if } x \in \mathcal{H} \\ -e^{-0.4}, & \text{if } x \notin \mathcal{H} \end{cases} \tag{25}$$

The CLBF $W(x)$ for the unbounded unsafe region is constructed with $\nu = -0.104$ and $\mu = 5000$.

Closed-loop simulations are run starting from various initial conditions of the two CSTRs inside the safety and stability regions under two scenarios: (1) in the presence of bounded, and (2) unbounded unsafe sets. The state trajectories of both CSTRs under CLBF-DMPC for cases of bounded and unbounded unsafe sets are shown in Figs. 1 and 2 respectively. These initial conditions are chosen to cover various points in state-space where the control problem becomes challenging to solve. For example, both CSTRs start at an initial condition very close to the boundary of the unsafe set, but at different positions such that the directions of state evolution may be different; one CSTR may start from the side of the unsafe set and the other CSTR may start from the side without the unsafe set, such that one MPC drives the closed-loop state of its respective subsystem around the unsafe ellipse, and the other MPC drives the closed-loop state of its subsystem towards the origin at optimal rate. It is demonstrated that the closed-loop system achieve stability while successfully avoiding the unsafe regions in both CSTRs when the simulation starts at the illustrated five initial conditions inside their respective regions $\mathcal{U}_{\rho_1}$ for CSTR-1 and $\mathcal{U}_{\rho_2}$ for CSTR-2, and eventually converges and is bounded in their respective terminal sets $\mathcal{U}_{\rho_{\min_1}}$ and $\mathcal{U}_{\rho_{\min_2}}$. This is shown for both scenarios of bounded and unbounded unsafe sets.

Note that we have selected initial conditions of the two CSTRs inside their respective stability and safety regions, $\mathcal{U}_{\rho_1}$ and $\mathcal{U}_{\rho_2}$, and the stability and safety region for the overall system $\mathcal{U}_\rho$ should be a subset of the union of the two individual sets, $\mathcal{U}_\rho \subseteq (\mathcal{U}_{\rho_1} \cup \mathcal{U}_{\rho_2})$. As it is difficult to have a closed-form representation of $\mathcal{U}_\rho$, the characterization of $\mathcal{U}_\rho$ can be carried out through numerical simulation to first find a region for which $\dot{W}(x, \Phi_1(x), \Phi_2(x)) < 0$, and then find the largest level set of $W(x)$ within this region.

The stability and safety region $\mathcal{U}_{\rho_1}$ for CSTR-1 can be characterized through numerical simulation by assessing $\dot{W}_1(x_1(t_k), \Phi_1(x_1(t_k)))$ and using information on the states of CSTR-1 itself. To rigorously characterize the stability and safety region $\mathcal{U}_{\rho_2}$ for CSTR-2, discretized points in state-space for which $\dot{W}_2(x(t_k), \Phi_2(x(t_k))) < 0$ need to be assessed first. However, since $x(t_k)$ also includes the $x_1(t_k)$, the characterization of $\mathcal{U}_{\rho_2}$ cannot be done without considering the process state of CSTR-1; this region can be also found via state-space discretization and extensive numerical simulations, but is difficult to visualize since it involves a 4-D state vector. Thus, considering bounded unsafe sets, Figs. 4 and 5 show some CSTR-2 points in state-space where $\dot{W}_2$ is rendered negative under the CLBF-based Sontag control law $\Phi_2(x)$ plotted with respect to x_1 of CSTR-1 and x_2 of CSTR-1 separately.

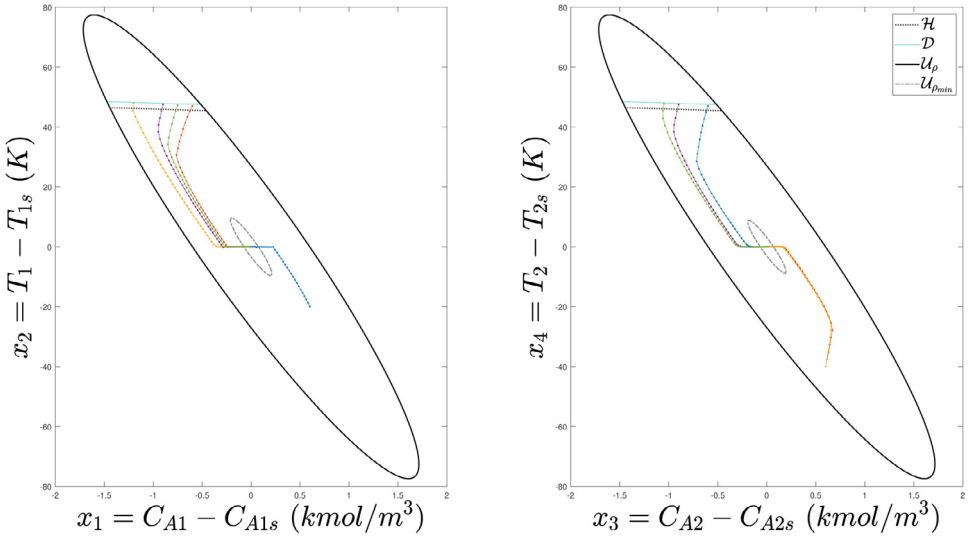

Fig. 2. Closed-loop trajectories of CSTR-1 and CSTR-2 under the sequential CLBF-DMPC in the presence of an unbounded unsafe set.

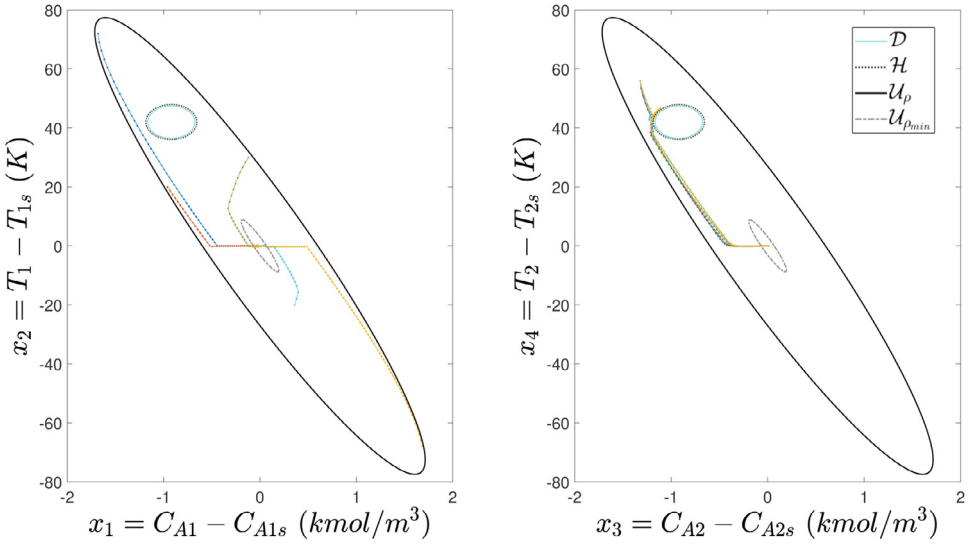

Fig. 3. Closed-loop trajectories starting from different initial conditions of CSTR-1 and the same initial condition of CSTR-2 under the sequential CLBF-DMPC in the presence of a bounded unsafe set showing safe and stable performance.

The x_1 and x_2 points of CSTR-1 are generated by discretizing $\mathcal{U}_{\rho_1}$, and the x_3 and x_4 points of CSTR-2 are generated by discretizing only the region in between the unsafe set $\mathcal{D}_2$ and the compact set $\mathcal{H}_2$ which encloses $\mathcal{D}_2$. We only assess discretized points in this critical region of safety to see which points may contribute to jeopardized safety when the states of CSTR-2 are near the boundary of the unsafe set. We can see that there exists combinations of (x_1, x_2) values that result in $\dot{W}_2 \geq 0$ under the CLBF-based Sontag control law $\Phi_2(x(t_k))$. In these situations, the CLBF-DMPC can still optimize for solutions of $u_{d_2}(x(t_k))$ that will yield decreasing W_2 along the predicted trajectory; for example, the constraint of Eq. (21h) can be activated and the set of discontinuous control actions $\bar{u}_2(x) \in U_2$ that exist to address the cases of saddle points can be used. In situations where $\dot{W}_2(x, \Phi_2(x)) = 0$, the existence of $\bar{u}_2(x) \in U_2$ ensure the feasibility of DMPC-2 in guaranteeing stability and safety. However, in situations where $\dot{W}_2(x, \Phi_2(x)) > 0$, DMPC-2 may run into points of in-feasibility during optimization and this is demonstrated in Fig. 6.

In this study, we only consider the set of initial conditions in the respective regions $\mathcal{U}_{\rho_1}$ and $\mathcal{U}_{\rho_2}$ for the closed-loop simulations of CSTR-1 and CSTR-2. In our simulations, $\mathcal{U}_{\rho_2}$ mirrors $\mathcal{U}_{\rho_1}$ for simplistic visualization and to provide a preliminary set of initial conditions for which we can consider to perform closed-loop control using the CLBF-DMPC. As such, we can demonstrate that there are certain values of states of CSTR-1 that may jeopardize closed-loop safety for the same valued CSTR-2 states under the explicit CLBF-based Sontag control law. Furthermore, even though the discontinuous control actions $\bar{u}_2(x) \in U_2$ ensure feasibility of the CLBF-DMPC and provide a set of solutions that decrease W_2 along the prediction trajectory in the neighborhood of saddle points where $\dot{W}_2 = 0$, there may be situations where $\dot{W}_2 > 0$ and DMPC-2 is unable to reach a feasible solution that decreases W_2 at that particular point in state-space. Fig. 3 demonstrates that starting from five different initial conditions of CSTR-1 within $\mathcal{U}_{\rho_1}$ and the same initial condition of CSTR-2 within $\mathcal{U}_{\rho_2}$, simultaneous stability and safety can be achieved for both CSTRs where the closed-loop states for the overall system do not enter the unsafe region and converges to the terminal sets. This demonstrates the efficacy of the CLBF-DMPC in handling the impact of the states of CSTR-1 on the closed-loop evolution of CSTR-2. We may also examine the

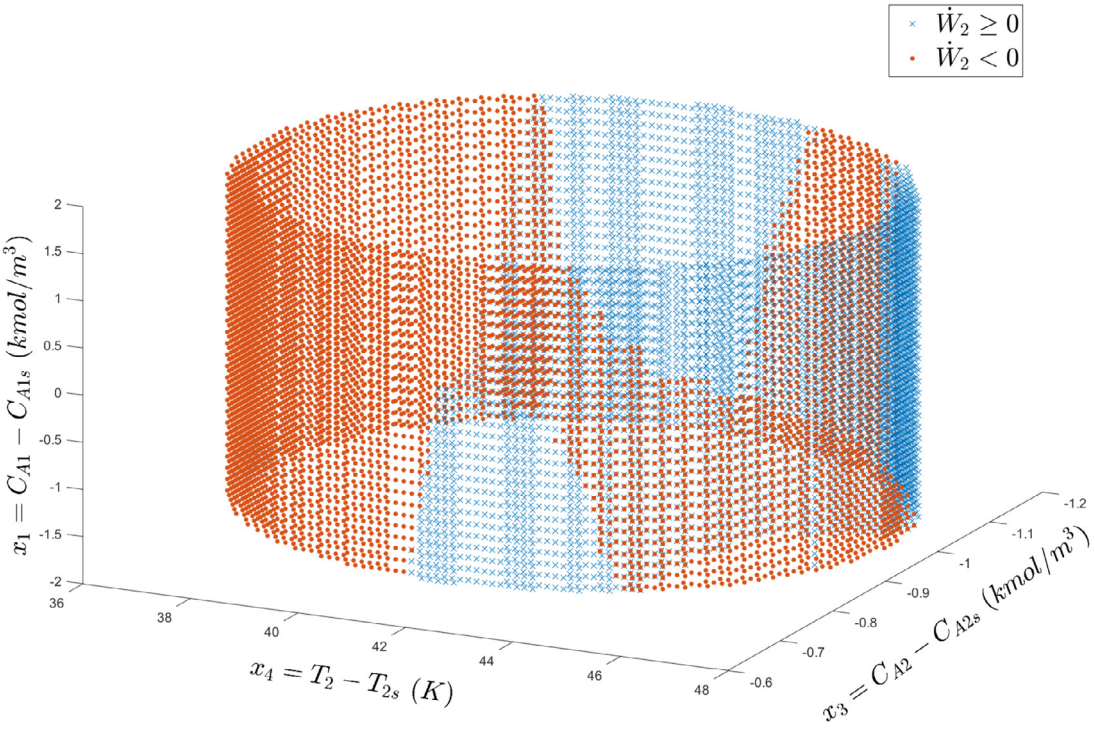

Fig. 4. Discretized points (x_3, x_4) near CSTR-2's unsafe region $\mathcal{D}_2$ in state-space showing the negativity and non-negativity of $\dot{W}_2$ under the CLBF-based Sontag control law with respect to different values of x_1 discretized from CSTR-1's safe operating region $\mathcal{U}_{\rho_1}$.

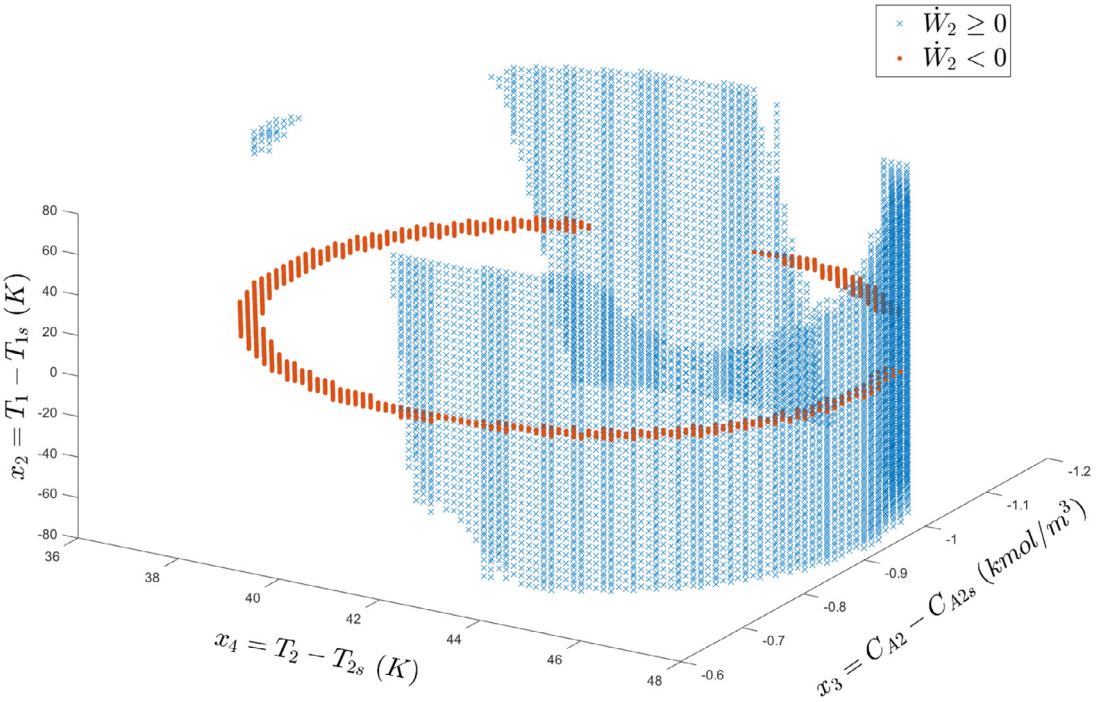

Fig. 5. Discretized points (x_3, x_4) near CSTR-2's unsafe region $\mathcal{D}_2$ in state-space showing the negativity and non-negativity of $\dot{W}_2$ under the CLBF-based Sontag control law with respect to different values of x_2 discretized from CSTR-1's safe operating region $\mathcal{U}_{\rho_1}$.

efficacy of CLBF-DMPC when the state of CSTR-2 is on the verge of critical safety. Starting from the same initial condition of CSTR-2 $(x_3,\ x_4) = (-1.135\ \text{kmol/m}^3,\ 45.2\ \text{K})$ that is within the enclosing compact set $\mathcal{H}_2$ but outside the unsafe set $\mathcal{D}_2$, we can see in Fig. 6 that some initial conditions of CSTR-1 (orange, $(x_1,\ x_2) = (-1.08\ \text{kmol/m}^3,\ 64\ \text{K})$) may result in safe closed-loop operation where the closed-loop state successfully avoids the unsafe sets $\mathcal{D}_1$ and $\mathcal{D}_2$, but some (blue, $(x_1,\ x_2) = (-0.6\ \text{kmol/m}^3,\ 36\ \text{K})$) may result in the closed-loop state of CSTR-2 entering the unsafe set $\mathcal{D}_2$. Note that both sets of initial conditions of CSTR-1 shown in Fig. 6 have been evaluated to have $\dot{W}_2(x, \Phi_2(x)) > 0$. However, it is shown that starting from $(x_1,\ x_2,\ x_3,\ x_4) = (-1.08\ \text{kmol/m}^3,\ 64\ \text{K},\ -1.135\ \text{kmol/m}^3,\ 45.2\ \text{K})$ (orange), the CLBF-DMPC is able to provide feasible so-

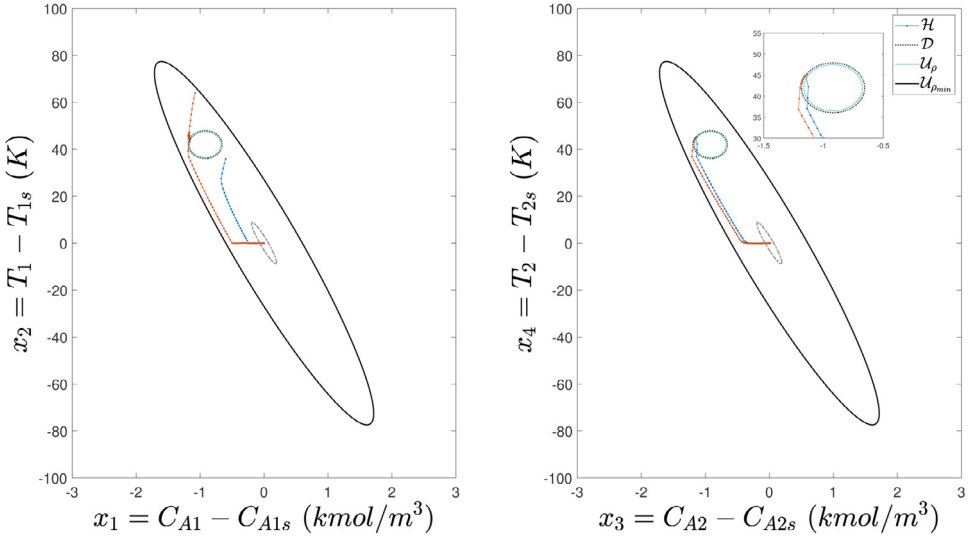

Fig. 6. Closed-loop trajectories starting from two different initial conditions of CSTR-1 and the same initial condition of CSTR-2 under the sequential CLBF-DMPC in the presence of a bounded unsafe set showing one safe (orange) and one unsafe (blue) trajectory.

lutions that yield $\dot{W}_2(x(t_k), u^*_{d_2}(t_k)) < 0$ and drive the closed-loop states away and around the unsafe set $\mathcal{D}_2$. On the other hand, starting from $(x_1,\ x_2,\ x_3,\ x_4) = (-0.6\ \text{kmol/m}^3,\ 36\ \text{K},\ -1.135\ \text{kmol/m}^3,\ 45.2\ \text{K})$ (blue), the CLBF-DMPC fails to provide a set of feasible solutions with $\dot{W}_2(x(t_k), u^*_{d_2}(t_k)) < 0$, therefore resulting in the closed-loop state of CSTR-2 entering the unsafe set $\mathcal{D}_2$ within the first sampling period.

7. Conclusion

We have shown theoretical analysis that nonlinear systems with input constraints and consisting of multiple subsystems can be stabilized by a CLBF-DMPC while not crossing the boundary of unsafe regions. A constrained CLBF is designed to characterize a stability region that has no intersection with the unsafe regions, and subsequently used to design CLBF-based explicit control laws for each subsystem. A CLBF-DMPC, which can be calculated either sequentially or iteratively, is presented and proven to have recursive feasibility as well as stability and safety properties with considerations of sample-and-hold control action implementation and presence of bounded disturbances. A modified DMPC structure is also studied and simulated for particular considerations of nonlinear subsystems. Lastly, the effectiveness of the proposed CLBF-DMPC system is demonstrated on a two-CSTR process with both bounded and unbounded unsafe sets.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Scarlett Chen: Conceptualization, Methodology, Software, Writing – original draft. **Zhe Wu:** Conceptualization, Methodology, Writing – original draft. **Panagiotis D. Christofides:** Writing – review & editing.

References

Chen, S., Wu, Z., Christofides, P., 2021. Cyber-security of centralized, decentralized, and distributed control-detector architectures for nonlinear processes. Chem. Eng. Res. Des. 165, 25–39.

Chen, S., Wu, Z., Christofides, P.D., 2022. Machine-learning-based construction of barrier functions and models for safe model predictive control. AIChE J. 68, e17456.

Chen, S., Wu, Z., Rincon, D., Christofides, P.D., 2020. Machine learning-based distributed model predictive control of nonlinear processes. AIChE J. 66, e17013.

Christofides, P.D., Scattolini, R., de la Pena, D.M., Liu, J., 2013. Distributed model predictive control: a tutorial review and future research directions. Comput. Chem. Eng. 51, 21–41.

Garcia, C.E., Prett, D.M., Morari, M., 1989. Model predictive control: theory and practicea survey. Automatica 25, 335–348.

Leveson, N., Stephanopoulos, G., 2014. A system-theoretic, control-inspired view and approach to process safety. AIChE J. 60. doi:10.1002/aic.14278.

Lin, Y., Sontag, E.D., 1991. A universal formula for stabilization with bounded controls. Syst. Control Lett. 16, 393–397.

Liu, J., Chen, X., Muñoz de la Peña, D., Christofides, P.D., 2012. Iterative distributed model predictive control of nonlinear systems: handling asynchronous, delayed measurements. IEEE Trans. Autom. Control 57 (2), 528–534.

Liu, J., Chen, X., Muñoz de la Peña, D., Christofides, P.D., 2010. Sequential and iterative architectures for distributed model predictive control of nonlinear process systems. Part I: theory. In: Proceedings of the 2010 American Control Conference. IEEE, Baltimore, MD, USA, pp. 3148–3155.

Marvi, Z., Kiumarsi, B., 2021. Safe reinforcement learning: a control barrier function optimization approach. Int. J. Robust Nonlinear Control 31, 1923–1940.

Qi, W., Liu, J., Christofides, P.D., 2013. Distributed supervisory predictive control of distributed wind and solar energy systems. IEEE Trans. Control Syst. Technol. 21 (2), 504–512. doi:10.1109/TCST.2011.2180907.

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

Sontag, E.D., 1989. A 'universal' construction of Artstein's theorem on nonlinear stabilization. Syst. Control Lett. 13, 117–123.

Stewart, B., Venkat, A., Rawlings, J., Wright, S., Pannocchia, G., 2010. Cooperative distributed model predictive control. Syst. Control Lett. 59, 460–469.

Venkat, A.N., Rawlings, J.B., Wright, S.J., 2004. Plant-wide optimal control with decentralized MPC. IFAC Proc. Vol. 37, 589–594.

Wächter, A., Biegler, L.T., 2006. On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. Math. Program. 106, 25–57.

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., 2019. Control Lyapunov-barrier function-based model predictive control of nonlinear systems. Automatica 109, 108508.

Wu, Z., Christofides, P.D., 2019. Handling bounded and unbounded unsafe sets in control Lyapunov-barrier function-based model predictive control of nonlinear processes. Chem. Eng. Res. Des. 143, 140–149.

Xu, X., Tabuada, P., Grizzle, J.W., Ames, A.D., 2015. Robustness of control barrier functions for safety critical control. IFAC-PapersOnLine 48 (27), 54–61.

Yang, X., Zhang, L., Xie, W., Zhang, J., 2019. Sequential and iterative distributed model predictive control of multi-motor driving cutterhead system for TBM. IEEE Access 7, 46977–46989.

Zeng, J., Zhang, B., Sreenath, K., 2021. Safety-critical model predictive control with discrete-time control barrier function. In: Proceedings of the 2021 American Control Conference (ACC). IEEE, New Orleans, LA, pp. 3882–3889.
Zhang, J., Liu, J., 2013. Distributed moving horizon state estimation for nonlinear systems with bounded uncertainties. J. Process Control 23, 1281–1295.
Zhang, Z., Wu, Z., Rincon, D., Garcia, C., Christofides, P.D., 2019. Operational safety of chemical processes via safeness-index based MPC: two large-scale case studies. Comput. Chem. Eng. 125, 204–215.