Journal of Loss Prevention in the Process Industries 53 (2018) 74–88

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Achieving operational process safety via model predictive control

Fahad Albalawi [b], Helen Durand [a], Anas Alanqar [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 Engineering, University of California, Los Angeles, CA 90095-1592, USA

ARTICLE INFO

Article history:
Received 5 September 2016
Received in revised form
2 October 2016
Accepted 30 November 2016
Available online 24 December 2016

Keywords:
Model predictive control
Chemical processes
Process control
Process functional safety
Process operation

ABSTRACT

Model predictive control (MPC) has been widely adopted in the chemical and petrochemical industry due to its ability to account for actuator constraints and multi-variable interactions for complex processes. However, closed-loop stability is not guaranteed within the framework of MPC without additional constraints or assumptions. An MPC formulation that can guarantee closed-loop stability in the presence of uncertainty is Lyapunov-based model predictive control (LMPC) which incorporates stability constraints based on a stabilizing Lyapunov-based controller. Though LMPC drives the closed-loop state trajectory to a steady-state, it lacks the ability to adjust the rate at which the closed-loop state approaches the steady-state in an explicit manner. However, there may be circumstances in which it would be desirable, for safety reasons, to be able to adjust this rate to avoid triggering of safety alarms or process shut-down. In addition, there may be scenarios in which the current region of operation is no longer safe to operate within, and another region of operation (i.e., a region around another steady-state) is appropriate. Motivated by these considerations, this work develops two novel LMPC schemes that can drive the closed-loop state to a safety region (a level set within the stability region where process functional safety is ensured) at a prescribed rate or can drive the closed-loop state to a safe level set within the stability region of another steady-state. Recursive feasibility and closed-loop stability are established for a sufficiently small LMPC sampling period. A comparison between the proposed method, which effectively integrates feedback control and safety considerations, and the classical LMPC method is demonstrated with a chemical process example. The chemical process example demonstrates that the safety-LMPC drives the closed-loop state into a safe level set of the stability region two sampling times faster than under the classical LMPC in the presence of process uncertainty.

1. Introduction

Process functional safety is critical to industrial chemical plants. The catastrophic incidents and disasters that have occurred over the past decades highlight the importance of safety and can be studied to prevent similar accidents in the future (Crowl and Louvar (2011)). These accidents may cause chemical substances to be released which can affect limited resources such as water and agricultural resources (Valipour (2012); Yannopoulos et al. (2015); Valipour and Singh (2016); Valipour (2016)). The frequency of accidents has motivated systematic methods for evaluating and improving process functional safety to be developed. For example, in (Leveson (2004)), an accident model is developed that can improve process functional safety. In (Kadri et al. (2014)), methods are developed to apply corrective actions based on data analysis, measurement and sorting processes to achieve meaningful process functional safety performance improvements. Process control is also utilized to control the risks that are associated with chemical processes (Bahr (2015)). Despite these methods for assessing and improving process functional safety, technological advances and further process/plant intensification continue to increase the complexity of maintaining safe process operation (Venkatasubramanian (2011); Leveson and Stephanopoulos (2014); Mannan et al. (2015)). Therefore, implementing control techniques that can predict and control the interactions between the components of these complex processes is necessary (Venkatasubramanian (2011)). In chemical plants, techniques such as hazards and operability (HAZOP) (Khan and Abbasi (2000); Dunjó et al. (2010)) analysis, fault trees and what-if scenarios are performed to evaluate the safety of a process. These techniques

* Corresponding author. 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).

http://dx.doi.org/10.1016/j.jlp.2016.11.021
0950-4230/

usually result in a report that describes the damage that would result from an accident. Chemical process safety has traditionally been addressed through process design decisions (e.g., designing the process to be inherently safe in terms of its chemistry and physics Kletz and Amyotte (2010); Gentile et al. (2003); Heikkilä et al. (1996)) and control and safety system design decisions (e.g., adding measurement sensors for critical process variables that trigger an alarm when an undesirable measurement is obtained).

Inherently safer designs are achieved through four primary principles: minimize (reduce the quantity of hazardous substances used and stored by a process), substitute (utilize less hazardous process chemistries), moderate (dilute chemicals or change operating conditions), and simplify (choose designs with less complexity and less potential to create hazardous conditions when faults or errors occur) Kletz (1985). Though designs can be made inherently safer, it is not possible to eliminate all hazards Kletz (2009), so a safety system, comprised of several independent layers, should be added to chemical processes. The layers of protection commonly used in industry are the basic process control system (BPCS), safety critical alarm system, safety trips/interlocks system, safety relief devices, containment and emergency response. Ideally, the layers of the safety system should not be activated regularly because a basic process control system (BPCS) regulates process variables to their set-points. When the control system is unable to keep the process variables within acceptable ranges due to, for example, equipment faults or unusually large process disturbances, alarms are triggered that alert operators to the issue so that actions can be taken to prevent further unsafe deviations. When operators are unable to bring the process back into a normal operating regime and the process variables exceed allowable values, the safety trips/interlocks system is triggered, which takes automatic and extreme actions such as forcing a valve to its fully open position to bring the process to a safer state of operation. Safety relief devices such as relief valves are used on vessels that can become highly pressurized very quickly, such that the control system, alarms, and safety trips/interlocks system would not be effective for preventing an explosion without the relief device. Containment is used to prevent hazardous material from entering the environment or injuring workers when the other layers of the safety hierarchy fail to prevent release of the material. The emergency response plan is used in severe cases that were not mitigated by any of the other layers of the safety hierarchy to minimize the impact to humans and the environment. The layers of the safety hierarchy are independent of each other and of the control system (i.e., they have separate sensors, computing elements, and actuators) to allow redundancy and improve safety Marlin (2012).

In (Leveson and Stephanopoulos (2014)), it has been argued that safety considerations can be used as constraints in control systems to combine process functional safety and process control in one framework. Nevertheless, the majority of the control techniques currently in use such as, for example, the traditional single-input/single-output (SISO) feedback control systems (e.g., PID controllers), would be incapable of enforcing safety constraints in the process control layer (Whiteley (2006)). Traditional SISO control strategies can be replaced with advanced control techniques that can potentially integrate safety and process control in one framework (Leveson and Stephanopoulos (2014)). One example of an advanced control system is tracking model predictive control (MPC), which is widely adopted in industry. MPC is a control technique that applies control actions (manipulated inputs) which are computed by formulating and solving a dynamic optimization problem on-line that takes advantage of a dynamic process model while accounting for process constraints (e.g., Mayne et al. (2000); Qin and Badgwell (2003); Mhaskar et al. (2006)). Several research works have integrated safety with MPC; for instance, an adaptive learning-based model predictive controller was designed to decouple safety and performance in an optimization framework (Aswani et al. (2013)) and a two-mode MPC with a standard mode and a reactive safety mode was designed to account for unexpected state-constraint changes (Carson et al. (2013)). In (Ahooyi et al. (2016)), a model-predictive safety system was developed that can detect operation hazards in a proactive fashion using model predictions to aid in safety alarm triggering. In addition, a recent research work has proposed data-based probabilistic models for special-cause event occurrences and operator response-times to evaluate the likelihood of alarm and safety interlock system failures (Moskowitz et al. (2016)).

Recently, a form of MPC termed Lyapunov-based model predictive control (LMPC) has gained attention (Mhaskar et al. (2006)) due to its guaranteed and explicit closed-loop stability properties in terms of characterization of the closed-loop stability region that the standard tracking MPC formulation with terminal stability constraints lacks. Though LMPC is guaranteed to drive the closed-loop state to a small neighborhood of the steady-state, the rate at which the LMPC drives the closed-loop state toward the equilibrium using a quadratic objective function and Lyapunov-based stability constraints alone may not be fast enough to ensure process functional safety. This can pose a safety issue if there are process transients that make it necessary for the closed-loop state to approach a safe level set of operation (safety region) around the steady-state more quickly and can lead to triggering safety alarms or process shutdown. Furthermore, quantifying *a priori* the rate at which the closed-loop state will move toward the safety region for a given tuning of the weighting matrices in the quadratic objective function is not possible in general, showing that adjusting the weighting matrices to achieve a required rate of approach to the safety region would not be sufficient.

Hence, it is necessary to develop an LMPC design that can adjust the rate at which the state approaches the safe operating region in unsafe scenarios. Moreover, the safe operating region may shift from a level set around one steady-state to a level set around another, and the LMPC should be able to drive the state to the newly computed safe operating region. However, the classical LMPC would be incapable of accomplishing this task because it is not designed to drive the closed-loop state to a safe operating region that corresponds to a new steady-state. To date, no work on formulating an MPC scheme that utilizes safety-based constraints, which controls the rate at which the closed-loop state approaches the steady-state in a direct manner, with guaranteed closed-loop stability properties, has been completed. Motivated by the above considerations, two LMPC schemes are first designed that can achieve safe operation of nonlinear processes by controlling the rate at which the closed-loop state moves toward a safe operating region which is associated with the original operating steady-state, and second, modifications to these LMPC schemes are developed that allow the closed-loop state to be driven to a level set within the stability region of another steady-state. Recursive feasibility and closed-loop stability of both safety-LMPC schemes are addressed for a sufficiently small LMPC sampling period. Using a chemical process example, the applicability of the proposed LMPC with safety-based constraints, which effectively integrates feedback control and safety considerations, is demonstrated and the performance is compared with that of a classical LMPC scheme.

2. Preliminaries

2.1. Notation

The transpose of a vector x is represented by the symbol x^T. The Euclidean norm of a vector is denoted by the operator $|\cdot|$. A level set

of a sufficiently smooth, positive definite scalar-valued function $V(x)$ is represented by the symbol Ω_ρ ($\Omega_\rho := \{x \in R^n : V(x) \leq \rho\}$). The symbol $S(\Delta)$ denotes the family of piecewise constant, right-continuous functions with period $\Delta \geq 0$. Set subtraction is denoted by the operator '/', that is, $A/B := \{x \in R^n : x \in A, x \notin B\}$.

2.2. Class of systems

Nonlinear process systems are considered with the following state-space description

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

where $x \in R^n$ is the state of the system, and $u \in R^m$ and $w \in R^w$ are the control (manipulated) input vector and the disturbance vector, respectively. The admissible input values are restricted to be in m nonempty convex sets $U_i \subseteq R$, $i = 1, \ldots, m$, defined as $U_i := \{u_i \in R : u_i^{\min} \leq u_i \leq u_i^{\max}\}$, where $u_i^{\max}$ and $u_i^{\min}$, $i = 1, \ldots, m$, are the magnitudes of the input constraints. The vector function f is assumed to be a locally Lipschitz vector function of its arguments with $f(0, 0, 0) = 0$. Further, the disturbance vector w is assumed to bounded within the set $W := \{w \in R^w : |w| \leq \theta, \theta > 0\}$ (i.e., $w \in W$).

2.3. Lyapunov-based controller assumption

The class of nonlinear systems of Eq. (1) is constrained to a class of stabilizable nonlinear systems. Particularly, the existence of a Lyapunov-based controller $h(x) = [h_1(x) \cdots h_m(x)]^T$ which renders the origin of Eq. (1) with $w(t) \equiv 0$ (the nominal closed-loop system) asymptotically stable with $h_i(x) \in U_i$, $i = 1, \ldots, m$, inside a given stability region Ω_ρ is assumed. Further, it is assumed that there exist (Massera (1956); Khalil (2002)) a sufficiently smooth Lyapunov function $V(x)$ for the nominal closed-loop system and class $\mathscr{K}$ functions $\alpha_i(\cdot)$, $i = 1, 2, 3, 4$, such that the following inequalities hold:

$$\begin{aligned} &\alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|) \\ &\frac{\partial V(x)}{\partial x} f(x, h_1(x), \ldots, h_m(x), 0) \leq -\alpha_3(|x|) \\ &\left|\frac{\partial V(x)}{\partial x}\right| \leq \alpha_4(|x|) \\ &h_i(x) \in U_i, i = 1, \ldots, m \end{aligned} \tag{2}$$

for all $x \in D \subseteq R^n$ where D is an open neighborhood of the origin. The stability region Ω_ρ of the process of Eq. (1) under $h(x)$ (where $\Omega_\rho \subseteq D$) is defined as a level set of the Lyapunov function within which $\dot{V}$ is negative. Designs for stabilizing control laws that account for input constraints for different classes of nonlinear systems have been developed (see, for instance, (Lin and Sontag (1991); Kokotović and Arcak (2001); El-Farra and Christofides (2003); Christofides and El-Farra (2005)).

When x is maintained within the compact set Ω_ρ, $u_i \in U_i$, $i = 1, \ldots, m$, and $w \in W$, we have from the continuity of x, the local Lipschitz property of f, and the smoothness of $V(x)$ that there exist positive constants M, L_x, L_w, L_x' and L_w' such that the following inequalities hold:

$$|f(x(t), u(t), w(t))| \leq M \tag{3}$$

$$|f(x, u, w) - f(x^*, u, 0)| \leq L_x|x - x^*| + L_w|w| \tag{4}$$

$$\left|\frac{\partial V(x)}{\partial x} f(x, u, w) - \frac{\partial V(x^*)}{\partial x} f(x^*, u, 0)\right| \leq L_x'\left|x - x^*\right| + L_w'\left|w\right| \tag{5}$$

for all $x, x^* \in \Omega_\rho$, $u_i \in U_i$, $i = 1, \ldots, m$, and $w \in W$.

2.4. Lyapunov-based model predictive control

Lyapunov-based model predictive control (LMPC) (Mhaskar et al. (2006)) is a model predictive control (MPC) strategy that incorporates Lyapunov-based constraints to ensure closed-loop stability of the optimization-based controller. The formulation of the classical LMPC optimization problem is as follows:

$$\min_{u(t) \in S(\Delta)} \int_{t_k}^{t_{k+N}} \left[\tilde{x}(\tau)^T Q \tilde{x}(\tau) + u(\tau)^T R u(\tau)\right] d\tau \tag{6a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{6b}$$

$$u(t) \in U, \forall t \in [t_k, t_{k+N}) \tag{6c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{6d}$$

$$V(\tilde{x}(t)) \leq \rho, \forall t \in [t_k, t_{k+N}) \tag{6e}$$

$$\begin{aligned} &\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \\ &\leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0) \end{aligned} \tag{6f}$$

where the decision variable of the optimization problem is the piecewise constant input trajectory $u(t)$. The input constraint of Eq. (6c) restricts the computed input trajectories to be within the admissible set over the prediction horizon. The nominal model of Eq. (1) is incorporated to predict the evolution of the system over the prediction horizon $N\Delta$ (Eq. (6b)). The notation $\tilde{x}(t)$ and $x(t_k)$ denotes the predicted state trajectory and the state measurement obtained at the sampling time t_k, respectively. The stage cost of the LMPC of Eq. (6) is a quadratic function that penalizes the deviations of the state and inputs from their corresponding steady-state values (Eq. (6a)). The weighting matrices Q and R are tuned to manage the trade-off between the amount of control energy required to move the state to the steady-state and the speed of approach to this steady-state (even though this trade-off is not transparent). Eqs. (6e) and (6f) represent the Lyapunov-based constraints where the constraint of Eq. (6e) maintains the closed-loop state of the process of Eq. (1) within the stability region Ω_ρ over the prediction horizon. Finally, the constraint of Eq. (6f) (contractive constraint) forces the time derivative of the Lyapunov function under the classical LMPC to be less than the time derivative of the Lyapunov function under the explicit stabilizing controller $h(x)$.

3. Safety-based LMPC design

In this section, an LMPC design is developed that incorporates safety-based constraints (termed safety-LMPC). In the first subsection, the motivation for adding safety-based constraints to the classical LMPC scheme of Eq. (6) is provided to form safety-LMPC. In the second and third subsections, the formulations of two proposed safety-LMPC optimization problems are given and the proofs of recursive feasibility and closed-loop stability of one of the safety-LMPC schemes are presented, with discussion of such properties for the other safety-LMPC scheme. In the fourth subsection, the changes required to the proposed safety-LMPC formulations to change the current region of operation to another one around a different steady-state are presented.

3.1. Motivation for safety-based constraints

Tracking MPC is widely used in the chemical process industries. The main purpose of tracking MPC is to steer the process to the operating steady-state and maintain process operation at this steady-state. However, in the presence of disturbances, tracking MPC does not guarantee closed-loop stability. Alternatively, the LMPC design of Eq. (6) uses the explicit stabilizing controller $h(x)$ to ensure closed-loop stability by decreasing the Lyapunov function value at the beginning of each sampling time. Though LMPC is thus able to guarantee closed-loop stability of the process, always maintaining process operation within Ω_ρ and driving the state to a neighborhood of the steady-state, there may be scenarios in which a region within Ω_ρ becomes unsafe to operate within. In this case, the closed-loop stability properties of LMPC, and the rate at which it drives the state to a neighborhood of the origin through the combination of the contractive constraint and tracking objective function, may not be enough to ensure safe process operation. The rate of approach to the steady-state is lower bounded by a worst-case rate at which $h(x)$ would drive the closed-loop state to the steady-state when implemented in sample-and-hold, but otherwise is determined by the weighting matrices Q and R and the penalties they place on deviations of the states and inputs from their steady-state values. The only flexibility this classical LMPC formulation offers for changing the rate of approach to the steady-state when process monitoring logic determines that the state needs to move to a smaller level set within the stability region quickly to avoid safety alarms or process shut-down is to adjust Q and R on-line. However, determining appropriate values of Q and R for a desired rate of approach to the safe region of operation is difficult. A method for enhancing the rate of approach to the steady-state when an unsafe situation is detected would allow the process control system to enhance process functional safety.

One method for improving the rate at which the closed-loop state approaches the steady-state is by shrinking the level set used within the LMPC formulation on-line when an unsafe situation is detected. A safe level set of the stability region $\Omega_{\rho_{sp}} \subset \Omega_\rho$, termed the safety region, could be identified, outside of which the enhanced rate of decrease would be imposed by shrinking the upper bound on $V(x)$ to force the state to enter smaller level sets at a desired rate. This would have the effect of forcing the state to move toward the origin at a rate potentially faster than that which would be achieved using the quadratic objective and contractive constraint alone. In this present work, two LMPC schemes are developed termed safety-LMPC 1 and safety-LMPC 2 that can enhance the rate at which the closed-loop state approaches $\Omega_{\rho_{sp}}$.

3.2. Safety-LMPC 1 formulation

Safety-LMPC 1 decreases the upper bound on the Lyapunov function with time to enhance the rate of approach of the closed-loop trajectories to the safety region by imposing a hard constraint within the LMPC scheme that decreases the upper bound on $V(x)$ at a fixed rate. The hard constraint, which can be utilized in place of Eq. (6e), is as follows:

$$V(\tilde{x}(t)) \leq \rho_{sp} + \Big(V(x(t_k)) - \rho_{sp}\Big)e^{-a(t-t_k)}, \quad \forall\, t \in [t_k, t_{k+N}) \tag{7}$$

where ρ_{sp} represents the safety set-point. The constant a represents the convergence rate, which can be assigned a value consistent with the rate of approach required to enter the safety region before safety issues occur (which may be a very large value if the required rate of approach is very fast). Based on the value of a, the closed-loop state is required to be within the safety region $\Omega_{\rho_{sp}}$ after a certain number of sampling times to satisfy the constraint. As a result of this constraint, the closed-loop state may enter the safety region more rapidly than under the classical LMPC design of Eq. (6). The proposed safety-LMPC 1 guarantees closed-loop stability of the system of Eq. (1) in the presence of uncertainty when the safety-LMPC 1 optimization problem is feasible; however, recursive feasibility is not guaranteed because the safety-based constraints may not satisfy the rate that the hard constraint of Eq. (7) requires (i.e., the parameter a is significantly large). When the closed-loop state enters $\Omega_{\rho_{sp}}$, the constraint of Eq. (7) can be replaced with the constraint of Eq. (6e) with $\rho = \rho_{sp}$.

Another idea for formulating safety-LMPC 1 with a hard upper bound on the rate of decrease of the Lyapunov function is to utilize a dynamic upper bound $\tilde{\rho}$ on $V(\tilde{x}(t_k))$ that also must meet Eq. (7) as follows:

$$\min_{u(t), K_c(t) \in S(\Delta)} \int_{t_k}^{t_{k+N}} \Big[\tilde{x}(\tau)^T Q \tilde{x}(\tau) + u(\tau)^T R u(\tau)\Big] d\tau \tag{8a}$$

$$\text{s.t.}\ \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{8b}$$

$$u(t) \in U,\ \forall\, t \in [t_k, t_{k+N}) \tag{8c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{8d}$$

$$K_c(t) \geq 0,\ \forall\, t \in [t_k, t_{k+N}) \tag{8e}$$

$$V(\tilde{x}(t)) \leq \tilde{\rho}(t) \leq \rho_{sp} + \Big(V(x(t_k)) - \rho_{sp}\Big)e^{-a(t-t_k)}, \quad \forall\, t \in [t_k, t_{k+N}) \tag{8f}$$

$$\frac{d\tilde{\rho}}{dt} = K_c(t)\Big(\rho_{sp} - \tilde{\rho}(t)\Big) \tag{8g}$$

$$\tilde{\rho}(t_k) = V(x(t_k)), \quad \text{if } x(t_k) \notin \Omega_{\rho_{sp}}$$

$$\tilde{\rho}(t_k) = \rho_{sp}, \quad \text{if } x(t_k) \in \Omega_{\rho_{sp}} \tag{8h}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0) \tag{8i}$$

where the notation follows that in Eq. (6). In addition to the manipulated input trajectory $u(t)$, the gain $K_c(t)$ is another decision variable that is restricted to take nonnegative values over the prediction horizon $N\Delta$ (Eq. (8e)). The performance index of the safety-LMPC 1 is the objective function of the classical LMPC of Eq. (6).

Eqs. (8e)–(8h) represent the safety-based constraints. The contractive constraint (Eq. (8i)) ensures that the closed-loop state enters $\Omega_{\rho_{sp}}$ in finite time by utilizing the explicit stabilizing controller $h(x)$ to compute control actions that decrease the value of the Lyapunov function at least as much as the decrease given by $h(x)$. Though the constraint of Eq. (8i) ensures that the closed-loop state of the process of Eq. (1) converges to the safety region $\Omega_{\rho_{sp}}$ at a rate that is at least as fast as that which the explicit stabilizing controller $h(x)$ would offer (it may be faster depending on Q and R), the role of the safety-based constraints is to enhance the rate of decrease of the state until it enters $\Omega_{\rho_{sp}}$ in the required number of

sampling times that the hard constraint of Eq. (8f) imposes, and then to resume the normal rate of approach to the steady-state using the classical LMPC scheme. This allows the original tuning of the objective function with respect to Q and R to retain its significance once the state is within a safe region of operation, and also allows for the rate of decrease toward the safety region to potentially be faster than it would be under the classical LMPC design alone. Specifically, the upper bound (Eq. (7)) in the constraint of Eq. (8f) enforces a fast rate of approach of the state to $\Omega_{\rho_{sp}}$ by causing the optimization problem to choose a K_c that will decrease the upper bound $\tilde{\rho}(t)$ on the Lyapunov function value of the predicted state as quickly as the rate of approach (parametrized by a) required to enter the safety region. This has the potential to decrease the level set of the predicted Lyapunov function value $V(\tilde{x}(t))$ over the prediction horizon more significantly than under the classical LMPC design alone, causing the closed-loop state to move more quickly toward the safety region $\Omega_{\rho_{sp}}$. The rate at which $\tilde{\rho}$ decreases is governed by the magnitude of the decision variable $K_c(t)$ in the first-order ordinary differential equation of Eq. (8g). Moreover, the predicted state trajectory $\tilde{x}(t)$ is maintained within the predicted level set $\Omega_{\tilde{\rho}(t)}$ over the prediction horizon by the constraint of Eq. (8f), so that the predicted state cannot leave $\Omega_{\tilde{\rho}}$ in a given prediction horizon once it enters it. To ensure that the classical LMPC design of Eq. (6) can be recovered when the optimization problem of Eq. (8) causes the state to enter $\Omega_{\rho_{sp}}$, the safety-LMPC utilizes state feedback to set the initial condition of the constraint of Eq. (8g) to the value of the Lyapunov function at the current state when the state measurement is outside the safety region $\Omega_{\rho_{sp}}$, or to the safety set-point ρ_{sp} if the current state enters the safety region (i.e., $x(t_k) \in \Omega_{\rho_{sp}}$) (Eq. (8h)). Thus, when $x(t_k)$ enters the safety region, the classical LMPC design is recovered because the constraint of Eq. (8g) will be set to zero and the bound of Eq. (7) is removed in Eq. (8f).

The constraint of Eq. (8f) may be more likely to become infeasible than the constraint of Eq. (7) because it requires that the dynamics of both the nominal process (Eq. (8b)) and the dynamics of $\tilde{\rho}$ (Eq. (8g)) cause Eq. (8f) to be met. However, the LMPC of Eq. (8) has the advantage of being more readily transformed to the soft constraint formulation that will be developed in the next subsection than does the LMPC formulation of Eq. (6) with Eq. (7) (and hence further discussion on this point will be deferred to that subsection). Despite the possible infeasibility of the safety-LMPC 1 formulation, the safety-based constraint allows it to require an explicit rate of decrease of the Lyapunov function value until the closed-loop state enters the safety region, which would be difficult to achieve by tuning Q and R if the safety-based constraints were not utilized.

Remark 1. The proposed safety-LMPC design does not study the process complexity itself (the nonlinear, coupled nature of the process dynamics is considered to be an innate aspect of the physics and chemistry of the process), rather this work is focused on the problem of the complexity (difficulty) of ensuring safe operation of nonlinear, highly coupled processes. The new solution proposed by this work is a control design that explicitly incorporates safety-based state constraints that guarantee recursive feasibility and closed-loop stability of a process under the controller, and also guarantee that the closed-loop process can be driven into a safe region of operation in finite time, under certain conditions. The new controller design proposed below can handle the difficulty associated with the conventional tracking MPC formulation in which it is not obvious how to adjust the matrices Q and R on-line so that the rate of approach to the steady-state when process monitoring logic determines that the state needs to move faster to a safe region of operation is enhanced. However, the proposed safety-LMPC design enhances the rate of approach to the steady-state by incorporating safety-based constraints and a safety penalty term that can shrink the level set used within the MPC formulation on-line. Subsequently, the process state will move toward the safe region of operation at a rate potentially faster than that which would be achieved using the quadratic objective function of the conventional tracking MPC. Thus, the proposed formulation avoids the difficulty of tuning the Q and R matrices due to safety considerations and can still achieve the goal of driving the closed-loop state to a region of operation closer to the steady-state at a faster rate than would otherwise be attained with the Q and R matrices unchanged.

Remark 2. It is noted that the safety-based constraints do not guarantee a decrease in the Lyapunov function value of the closed-loop state at the rate given by Eq. (8g) because the dynamics of $V(x)$ are not those in Eq. (8g) and furthermore process disturbances will cause the value of $V(x)$ along the actual closed-loop state trajectory to differ from the predicted upper bound in Eq. (8). However, when $K_c(t)$ and $u(t)$ decrease $\tilde{\rho}(t)$ significantly, it is possible that the actual process state will move significantly closer to the safety region for that same value of the input, which may cause the closed-loop state under Eq. (8) to be driven into $\Omega_{\rho_{sp}}$ more quickly than it would be under Eq. (6).

Remark 3. Though $K_c(t)$ is piecewise constant with period Δ in Eq. (8), it is not a physical quantity and thus could be piecewise constant with a different period if desired.

Remark 4. Though it is possible to continue to enforce the enhanced rate of decrease to the steady-state from Eqs. (7 or 8f) even after the closed-loop state enters $\Omega_{\rho_{sp}}$, this would not in general be desirable because the weighting matrices Q and R are typically chosen to allow a trade-off between the rate of approach to the steady-state and the use of the inputs. If the safety-based constraints of the safety-LMPC were always active and drove the state quickly toward the origin, Q and R would lose their value as tuning parameters because the effect would be like having a large Q.

Remark 5. An alternative upper bound in Eqs. (7) and (8f) is $(\rho_{sp} + (V(x(t_{saf})) - \rho_{sp})e^{-a(t-t_{saf})})$, where t_{saf} corresponds to the time at which process monitoring logic requests that the closed-loop state begin to move toward the safety region. This upper bound ensures that the only change in the value of the upper bound is due to t increasing, whereas the upper bound in Eqs. (7) and (8f) changes not only due to t changing, but also due to changes in $V(x(t_k))$ and t_k. Thus, the requested rate of decrease toward the safety region corresponding to the former upper bound may be more easily understood a priori using the decaying exponential, whereas it is more difficult to determine the rate of decrease throughout time with the latter upper bound because at any given sampling period it depends on the process state measurement $x(t_k)$, which is affected by prior chosen control actions and process disturbances that cannot be known a priori.

3.3. Safety-LMPC 2 formulation

The second safety-LMPC formulation that is proposed in this work is a modification of the formulation of safety-LMPC 1 such that the resulting controller, termed safety-LMPC 2, forces the closed-loop state to go to $\Omega_{\rho_{sp}}$ while recursive feasibility and closed-loop stability of the process of Eq. (1) under safety-LMPC 2 are guaranteed. The mathematical formulation of safety-LMPC 2 for the process of Eq. (1) is as follows:

$$\min_{u(t),K_c(t)\in S(\Delta)} \int_{t_k}^{t_{k+N}} \left[\tilde{x}(\tau)^T Q\tilde{x}(\tau) + u(\tau)^T Ru(\tau) + \phi\left(\rho_{sp} - \tilde{\rho}(\tau)\right)\right] d\tau \tag{9a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{9b}$$

$$u(t)\in U,\ \forall t\in[t_k, t_{k+N}) \tag{9c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{9d}$$

$$K_c(t) \geq 0,\ \forall t\in[t_k, t_{k+N}) \tag{9e}$$

$$V(\tilde{x}(t)) \leq \tilde{\rho}(t),\ \forall t\in[t_k, t_{k+N}) \tag{9f}$$

$$\frac{d\tilde{\rho}}{dt} = K_c(t)\left(\rho_{sp} - \tilde{\rho}(t)\right) \tag{9g}$$

$$\tilde{\rho}(t_k) = V(x(t_k)), \quad \text{if } x(t_k)\notin\Omega_{\rho_{sp}}$$

$$\tilde{\rho}(t_k) = \rho_{sp}, \quad \text{if } x(t_k)\in\Omega_{\rho_{sp}} \tag{9h}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0) \tag{9i}$$

where the notation follows that in Eq. (8). The performance index of the safety-LMPC 2 formulation includes the objective function of the classical LMPC of Eq. (6) and a safety penalty term. The safety penalty term $\phi(\rho_{sp} - \tilde{\rho}(t))$ penalizes the deviation of the upper bound of the Lyapunov function value $\tilde{\rho}(t)$ from the safety set-point ρ_{sp} over the prediction horizon. Specifically, the penalty term in the objective can be appropriately weighted to enforce a fast rate of approach of the state to $\Omega_{\rho_{sp}}$ by causing the optimization problem to choose a K_c that will decrease the upper bound $\tilde{\rho}(t)$ on the Lyapunov function value of the predicted state rapidly. This has the potential to decrease the value of the Lyapunov function along the predicted closed-loop state trajectories ($V(\tilde{x}(t))$) over the prediction horizon more significantly than under the classical LMPC design alone, causing the closed-loop state to move more quickly toward the safety region $\Omega_{\rho_{sp}}$. However, the rate of decrease to the safety region does not necessarily meet the convergence rate required by Eq. (7) because safety-LMPC 2 enforces the hard constraint of Eq. (7) as a soft constraint through a penalty term in the objective function to drive the closed-loop state to $\Omega_{\rho_{sp}}$ while feasibility of the optimization problem is guaranteed for all times.

It was noted in the prior section that the benefits of the dynamic upper bound $\tilde{\rho}$ utilized within the safety-LMPC 1 formulation in Eq. (8) (as opposed to the formulation of Eq. (6) with Eq. (7)) would be more clear after the formulation of safety-LMPC 2 had been introduced, and they will now be discussed. Specifically, the formulation of Eq. (8) clarifies the relationship between the desired rate of approach to the safety region as parametrized by a and the gain K_c calculated by the LMPC (i.e., a specific gain K_c must be chosen in any given sampling period if the rate of approach parameterized by a is to be met in Eq. (8f)). This is helpful in understanding how the rate of approach to the steady-state is embedded within the soft constraint formulation of Eq. (9) through the gain K_c. Furthermore, the closeness of the formulations of Eqs. (8) and (9) is beneficial because it provides a strategic set-up for, for example, employing logic that enforces a specific rate of decrease through Eq. (8) when that optimization problem is feasible but then switches to the soft constraint formulation of Eq. (9) with minimal adjustment of the optimization problem when Eq. (8) becomes infeasible (i.e., only a penalty on the objective function and the removal of the upper bound on $\tilde{\rho}$ in Eq. (8f) need to be implemented when infeasibility occurs to obtain a control action that can guarantee closed-loop stability and controller feasibility; the transition to the modified optimization problem is not as smooth with the formulation of Eq. (6) with Eq. (7), for which new constraints and optimization variables would need to be added to the optimization problem to enable the transition).

Safety-LMPC 2 provides two primary benefits in terms of enforcing the rate of approach of the closed-loop state to the safety region that cannot easily be obtained by tuning Q and R in an LMPC formulation without safety-based constraints. Firstly, safety-LMPC 2 may aid as noted in the previous paragraph in developing a controller design that can easily transition between the LMPC formulation of Eq. (8) and that of Eq. (9) whenever Eq. (8) becomes infeasible to encourage the closed-loop state to meet the explicit rate of approach to the safety region (that could not easily be determined by adjusting Q and R) that is enforced by Eq. (8f) as closely as possible. Furthermore, even if safety-LMPC 2 is utilized on its own (i.e., not with Eq. (8)), safety-LMPC 2 still allows for one parameter (the weighting on the penalty on $(\rho_{sp} - \tilde{\rho})$ in the objective function) to be adjusted to alter the rate of approach to the safety region as desired. When it is unclear how large this weight should be for a desired rate of approach, it can be adjusted based on process data. Specifically, the rate at which the closed-loop state moves toward the safety region can be evaluated based on measurements of the process state between sampling times. Then, based on whether this rate is appropriate for the safety concerns at hand, the weight can be increased (to drive the process state toward the safety region more quickly) or decreased (if the rate is faster than required and is using more control action than desired). The relative weighting on the safety penalty term compared to the quadratic terms in the objective function may depend on the process dynamics and the length of time remaining until it is desired that the state be within the safety region. This allows the difficult problem of adjusting Q and R at the same time (which involves not just tuning two different quantities with respect to one another, but also all of the individual values within both matrices) to achieve a desired rate of approach to the safety region to be simplified to the problem of adjusting only one parameter, the weighting on the penalty term.

Remark 6. The main objective of our work is to enhance the safety performance of the conventional tracking MPC by imposing safety-based constraints and Lyapunov-based constraints into the MPC so that the process state variables can be driven to the safety region at a faster rate than the conventional tracking MPC would offer. The safety region is defined as a level set of the stability region where the process state variables stay within a range that prevents triggering of safety alarms. Similar to the conventional tracking MPC, the proposed safety-LMPC can be applied to nonlinear systems that do not obey the superposition principle which defines linear systems. Our scope includes the nonlinear processes and it also includes a number of assumptions regarding process safety, such as that there are no actions from the safety system interfering with the actions of the control system, and that the region of safe operation can be pre-determined on-line as a level set. Also, this work considers controlling a nonlinear process (in terms of its dynamics, the underlying differential equations describing the physico-chemical phenomena are nonlinear ordinary differential equations) with an MPC that includes safety constraints. MPC's should be equipped

with a sufficiently accurate process model to provide accurate state predictions; in this work, it is considered that the MPC includes a nonlinear process model to make state predictions. It is in that sense that the MPC incorporates nonlinearity (i.e., the MPC determines optimal control actions to apply based on how it predicts these control actions will affect the state of a nonlinear process throughout the prediction horizon, and also the control actions are applied to a nonlinear process). Therefore, LMPC is a nonlinear controller as it has constraints and uses a nonlinear model to compute control actions that regulate the nonlinear process state - LMPC is not a linear controller.

3.3.1. Feasibility and stability analysis of safety-LMPC 2

In this subsection, sufficient conditions are presented such that the state of the closed-loop system of Eq. (1) under the safety-LMPC 2 design is guaranteed to enter the safety region $\Omega_{\rho_{sp}}$ in finite time and reside within the safety region $\Omega_{\rho_{sp}}$ thereafter. Moreover, it is proved that the closed-loop state is guaranteed to be ultimately bounded within a compact set containing the origin. Because safety-LMPC 1 is not guaranteed to be recursively feasible but safety-LMPC 2 is, the feasibility and stability analysis is only presented for safety-LMPC 2, though the closed-loop stability results also hold for both safety-LMPC 1 formulations (Eq. (6) with Eq. (7) and Eqs. (8a)–(i)) when those formulations are recursively feasible. The following theorem provides sufficient conditions that prove practical stability of the system of Eq. (1) under the proposed safety-LMPC 2 design.

Theorem 1. Consider the system of Eq. (1) in closed-loop under the safety-LMPC 2 design of Eqs. (9a)–(i) based on a controller $h(x)$ that satisfies the conditions of Eq. (2). Let $\varepsilon_w > 0$, $\Delta > 0$, $\rho > \rho_{sp} > \rho_s > 0$ satisfy

$$-\alpha_3\left(\alpha_2^{-1}(\rho_s)\right) + L_x' M\Delta + L_w'\theta \leq -\varepsilon_w/\Delta. \tag{10}$$

If $x(t_0) \in \Omega_\rho$, $\rho_{\min} \leq \rho$ and $N \geq 1$ where

$$\rho_{\min} = \max\{V(x(t+\Delta)) : V(x(t)) \leq \rho_s\}, \tag{11}$$

then the closed-loop state $x(t)$ of Eq. (1) is guaranteed to enter the safety region $\Omega_{\rho_{sp}}$ in finite time and then reside there, and also the state $x(t)$ of the closed-loop system is ultimately bounded in $\Omega_{\rho_{\min}}$.

Proof. The proof consists of two parts. The first part includes the proof of the feasibility of the safety-LMPC 2 optimization problem for all states $x(t) \in \Omega_\rho$. The second part includes the proof of the two results of Theorem 1.

Part 1: The proposed safety-LMPC 2 of Eq. (9) is always a feasible optimization problem. The feasibility of the safety-LMPC 2 formulation is guaranteed because the following solution is always feasible:

$$\begin{aligned} &K_c(t) = 0, \ \forall\ t \in [t_k, t_{k+N}) \\ &u(t) = h(\tilde{x}(t_n)), \ \forall\ t \in [t_n, t_{n+1}) \\ &\text{with } n = k, \ldots, N+k-1, \ \forall\ \tilde{x}(t) \in \Omega_\rho \end{aligned} \tag{12}$$

The proof of feasibility of the solution of Eq. (12) is given in four steps: 1) the gain $K_c(t) = 0, \forall t \in [t_k, t_{k+N})$ is feasible since it satisfies Eq. (9e) over the prediction horizon 2) when $K_c(t) = 0$ throughout the prediction horizon, then by Eq. (9g), $\tilde{\rho}(t)$ will be equal to its initial value from Eq. (9h) throughout the prediction horizon, and hence the upper bound on the Lyapunov function in Eq. (9f) will remain constant (i.e., either $\tilde{\rho}(t_k) = V(x(t_k)) \Rightarrow V(\tilde{x}(t)) \leq V(x(t_k)), \forall t \in [t_k, t_{k+N})$, if $x(t_k) \notin \Omega_{\rho_{sp}}$ or $\tilde{\rho}(t_k) = \rho_{sp} \Rightarrow V(\tilde{x}(t)) \leq \rho_{sp}, \forall t \in [t_k, t_{k+N})$ if $x(t_k) \notin \Omega_{\rho_{sp}}$) 3) when $\tilde{\rho}$ is constant, the feasibility of $u(t) = h(\tilde{x}(t_n)), \forall t \in [t_n, t_{n+1})$, with $n = k, \ldots, N+k-1$, is guaranteed because it satisfies the input constraint of Eq. (9c) and also, because of the closed-loop stability property of the Lyapunov-based controller $h(x)$ (Muñoz de la Peña and Christofides (2008)), it satisfies the constraint of Eq. (9f) and (4)) finally, $u(t) = h(\tilde{x}(t_n)), \forall t \in [t_n, t_{n+1})$, with $n = k, \ldots, N+k-1$, satisfies the contractive constraint of Eq. (9i) making it a feasible input trajectory for the safety-LMPC 2 design. Therefore, the solution of Eq. (12) is a feasible solution, and recursive feasibility of the safety-LMPC 2 follows if the closed-loop state trajectory is maintained within Ω_ρ.

Part 2: In this part, it is proved that if the closed-loop state $x(t_k)$ is initialized within the stability region, but outside the safety region (i.e., $x(t_k) \in \Omega_\rho / \Omega_{\rho_{sp}}$), then within finite time the closed-loop state will enter the safety region $\Omega_{\rho_{sp}}$, and also will be ultimately bounded in a small region containing the origin $\Omega_{\rho_{\min}}$.

If $x(t_k) \in \Omega_\rho / \Omega_{\rho_s}$, then due to the contractive constraint of Eq. (9i) in the safety-LMPC 2 formulation of Eq. (9), the Lyapunov function of the closed-loop state will decrease for the first sampling period in the prediction horizon by at least the worst-case rate given by the explicit stabilizing controller $h(x)$. Owing to the closed-loop stability property of the explicit controller $h(x)$ (Muñoz de la Peña and Christofides (2008)), the Lyapunov function value of the closed-loop state under the safety-LMPC design will decrease in the next sampling period (i.e., $V(x(t)) \leq V(x(t_k)), \forall t \in [t_k, t_{k+1})$, which is derived in (Heidarinejad et al. (2012))). Thus, if $x(t_k) \in \Omega_\rho / \Omega_{\rho_s}$ then $V(x(t_{k+1})) < V(x(t_k))$ and in finite time, the closed-loop state converges to Ω_{ρ_s} (i.e., $x(t_{k+j}) \in \Omega_{\rho_s}$ where j is a finite positive integer). By the definitions of ρ_s and $\rho_{\min}$ in Theorem 1, once the closed-loop state converges to $\Omega_{\rho_s} \subseteq \Omega_{\rho_{\min}}$, it remains inside $\Omega_{\rho_{\min}}$ for all times. This proves the second result of Theorem 1 which is the ultimate boundedness of the closed-loop state in $\Omega_{\rho_{\min}}$. However, the first result of Theorem 1 which is that the closed-loop state converges to the safety region $\Omega_{\rho_{sp}}$ in finite time and then resides there is a result of the previous proof due to the assumption that $\rho_{sp} > \rho_s$ which is stated in Theorem 1.

3.4. Safety region changes

The safety-LMPC formulations of Eq. (6) with Eq. (7) and of Eqs. (8) and (9) assume that $\Omega_{\rho_{sp}}$ is a subset of Ω_ρ. However, there may be scenarios in which the safety logic unit indicates that regions within the current stability region Ω_ρ are no longer safe to operate within, but that another safety region that is a subset of a different stability region is appropriate. Therefore, it is necessary to modify the safety-LMPC during the transition between the stability regions in a manner that allows the region of operation to shift. The manner in which the safety-based LMPC formulation should be modified depends on the configuration of the old stability and safety regions (Ω_{ρ_1} and $\Omega_{\rho_{sp1}}$ respectively) with respect to the newly requested stability and safety regions (Ω_{ρ_2} and $\Omega_{\rho_{sp2}}$ respectively). This will be illustrated by presenting two example configurations in the context of the safety-LMPC 2 of Eq. (9), though the closed-loop stability results noted will also hold for the safety-LMPC 1 formulations of Eq. (6) with Eq. (7) and of Eq. (8) when those LMPC's are feasible.

Fig. 1 shows one possible configuration (Configuration 1) of the two different safe regions of operation $\Omega_{\rho_{sp1}}$ and $\Omega_{\rho_{sp2}}$. For this configuration, the safety-LMPC 2 of Eq. (9) will be applied with $\rho_{sp} = \rho_{sp1}$ until the closed-loop state enters $\Omega_{\rho_{sp1}}$. At the switching time t_s, the safety logic unit determines that $\Omega_{\rho_{sp2}}$ is the new safe

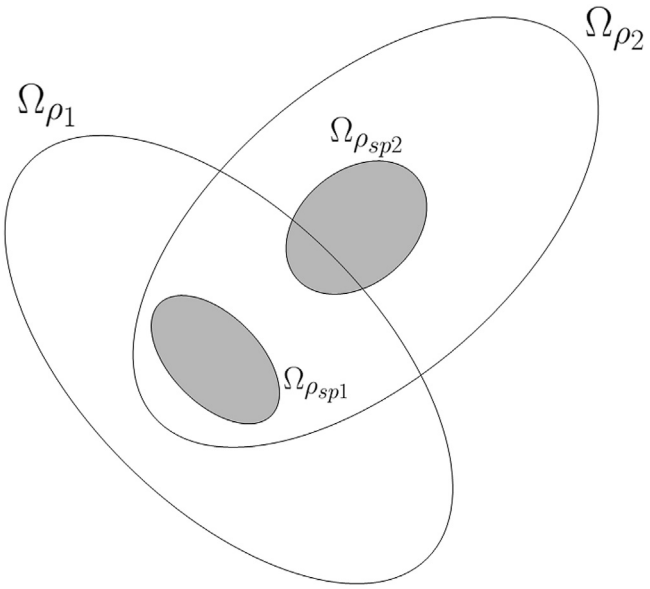

Fig. 1. Configuration 1 for switching between two different safe regions of operation.

region of operation, which is a subset of the stability region Ω_{ρ_2}. Therefore, at this time ρ_{sp} in the formulation of Eq. (9) will be changed to ρ_{sp2} (the quadratic terms in the objective function, nominal process model, and Lyapunov function will also be reformulated to have their origins at the new steady-state). Because the first safety region $\Omega_{\rho_{sp1}}$ is contained within the stability region Ω_{ρ_2} and the safety-LMPC 2 of Eq. (9) with $\rho_{sp} = \rho_{sp2}$ drives the closed-loop state into $\Omega_{\rho_{sp2}}$ from any initial condition in Ω_{ρ_2}, the safety-LMPC 2 of Eq. (9) is feasible after t_s and guarantees that the closed-loop state will be driven from $\Omega_{\rho_{sp1}}$ into $\Omega_{\rho_{sp2}}$ in finite time.

Fig. 2 shows a second possible configuration (Configuration 2) of Ω_{ρ_1}, $\Omega_{\rho_{sp1}}$, Ω_{ρ_2}, and $\Omega_{\rho_{sp2}}$. In this case, $\Omega_{\rho_{sp1}}$ is not fully within the stability region Ω_{ρ_2}. To drive the closed-loop state from any initial condition within $\Omega_{\rho_{sp1}}$ into $\Omega_{\rho_{sp2}}$ after t_s, one method is to remove the constraints of Eqs. (9e)–(9i) and the safety penalty term in the objective function (formulated with $\rho_{sp} = \rho_{sp1}$) from Eq. (9) at t_s, and to instead utilize a terminal region constraint (e.g., $\tilde{x}(t_{s+\overline{N}}) \in \Omega_{\rho_2}$) with a sufficiently long prediction horizon $\overline{N}$ to drive the closed-loop state into Ω_{ρ_2} by the end of the prediction horizon.

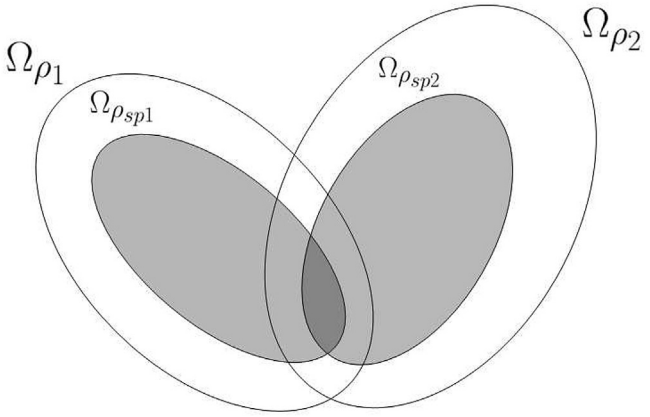

Fig. 2. Configuration 2 for switching between two different safe regions of operation.

However, due to the hard terminal constraint, feasibility of this optimization problem is not guaranteed. The formulation of the proposed safety-LMPC for the process of Eq. (1) to be used during the transition from $\Omega_{\rho_{sp1}}$ to Ω_{ρ_2} is as follows:

$$\min_{u(t)\in S(\Delta)} \int_{t_k}^{t_{k+\overline{N}}} \left[\tilde{x}(\tau)^T Q \tilde{x}(\tau) + u(\tau)^T R u(\tau)\right] d\tau \tag{13a}$$

$$\text{s.t.}\, \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{13b}$$

$$u(t) \in U,\ \forall\, t \in \left[t_k, t_{k+\overline{N}}\right) \tag{13c}$$

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

$$V_2(\tilde{x}(t)) \le \rho_2,\ \forall\, t \in \left[t_{s+\overline{N}}, t_{k+\overline{N}}\right] \tag{13e}$$

$$V_1(\tilde{x}(t)) \le \rho_1,\ \forall\, t \in \left[t_k, t_{s+\overline{N}}\right) \tag{13f}$$

where the objective function, nominal process model, and Lyapunov function V_1 for the old steady-state have their minimums at the original steady-state, but the Lyapunov function V_2 for the new steady-state has its origin at the new steady-state. In the transitioning period, the terminal region constraint of Eq. (13e) will be activated with a sufficiently long prediction horizon $\overline{N}$ to force the closed-loop state to be within the second stability region Ω_{ρ_2} at the end of the prediction horizon $t_{s+\overline{N}}$. If the closed-loop state is outside the second stability region Ω_{ρ_2} at the switching time t_s, feasibility of the proposed controller of Eq. (13) is not guaranteed. The Lyapunov-based constraint of Eq. (13f) is imposed to guarantee that the closed-loop state chooses a path that does not go outside the first stability region Ω_{ρ_1} to maintain closed-loop stability of the process in the transitioning period. In other words, the closed-loop state will be driven to the intersection between the two stability regions Ω_{ρ_1} and Ω_{ρ_2}. After that, the safety-LMPC of Eq. (8) will be applied with $\rho_{sp} = \rho_{sp2}$ and the objective function, Lyapunov function, and nominal process model with their origins at the new steady-state to drive the closed-loop state into the safety region $\Omega_{\rho_{sp2}}$.

An alternative method for attempting the safety region transition is to remove the contractive constraint from Eq. (9) at t_s and to add a soft constraint (e.g., a penalty on $(V(\tilde{x}(t)) - \rho_2)$) in the objective function to encourage the LMPC to compute control actions that drive the closed-loop state into Ω_{ρ_2}. Though this approach would always be feasible, there is still no guarantee that the state will be driven into Ω_{ρ_2}. However, once the state enters Ω_{ρ_2}, the LMPC problem of Eq. (9) with $\rho_{sp} = \rho_{sp2}$ and the appropriate modifications to the objective function, f, and V could be used to drive the state into $\Omega_{\rho_{sp2}}$. These two example configurations show that the manner in which Ω_{ρ_1}, $\Omega_{\rho_{sp1}}$, Ω_{ρ_2}, and $\Omega_{\rho_{sp2}}$ are related to each other (e.g., how they intersect) determines how the safety-LMPC 2 of Eq. (9) should be modified at t_s until the state enters Ω_{ρ_2} to drive the state into the new stability region, and also whether this can be achieved while guaranteeing closed-loop stability and feasibility.

4. Application to a chemical process example

To illustrate the safety advantage of the safety-LMPC paradigm over the classical LMPC, a chemical process example is considered which is a well-mixed, non-isothermal continuous stirred tank reactor (CSTR). The reaction transforms a reactant A to a product B

through an irreversible, exothermic second-order reaction $A \rightarrow B$. The feed of the CSTR consists of pure A and the inlet concentration of A is C_{A0}. The inlet temperature and feed volumetric flow rate of the reactor are T_0 and F, respectively. By applying material and energy balances under standard modeling assumptions, the concentration of A (C_A) and temperature T are modeled as follows:

$$\frac{dC_A}{dt} = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{RT}} C_A^2 \tag{14a}$$

$$\frac{dT}{dt} = \frac{F}{V}(T_0 - T) + \frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{RT}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{14b}$$

The notation ΔH, k_0, E, and R represent the enthalpy of reaction, pre-exponential constant, activation energy, and ideal gas constant, respectively. The reactor volume V, heat capacity C_p, and fluid density ρ_L within the reactor are assumed constant. Table 1 shows the values of the process parameters used in the simulations. The dynamic model of Eqs. (14a) and (b) is numerically simulated by using the explicit Euler method with an integration time step of $h_c = 10^{-5}$ hr.

The two states of the CSTR are C_A and T, and the two manipulated inputs are C_{A0} and Q. In this simulation, the safety-LMPC 2 of Eq. (9) is applied to the closed-loop CSTR due to its guaranteed closed-loop stability and recursive feasibility properties in the presence of uncertainty. The process of Eq. (14) is operated at an unstable steady-state $[C_{As}\ T_s] = \left[2\ \frac{kmol}{m^3}\ 400\ K\right]$ with associated steady-state input values $[C_{A0s} Q_s] = \left[4\ \frac{kmol}{m^3} 0\ \frac{kJ}{hr}\right]$ to demonstrate the ability of the safety-LMPC 2 to enhance process functional safety even around open-loop unstable operating points. The nonlinear process of Eq. (14) can be formulated as the following class of nonlinear systems

$$\dot{x}(t) = \tilde{f}(x(t)) + g_1(x(t))u_1(t) + g_2(x(t))u_2(t) \tag{15}$$

where $x(t)$ and $u(t)$ denote the state and the manipulated inputs of the CSTR in deviation variable form (i.e., $x^T = [C_A - C_{As}\ T - T_s]$ is the state vector and $u^T = [C_{A0} - C_{A0s}\ Q - Q_s]$ is the manipulated input vector), $\tilde{f}^T = [\tilde{f}_1\ \tilde{f}_2]$ is a vector containing the terms in the CSTR model that do not include u_1 or u_2, and $g_i^T = [g_{i1}\ g_{i2}]$ $(i = 1, 2)$ is a vector containing the terms in the CSTR model that multiply u_1 (for $i = 1$) or u_2 (for $i = 2$). The magnitudes of the manipulated inputs are bounded as follows: $\left|u_1\right| \leq 3.5\ \frac{kmol}{m^3}$ and $\left|u_2\right| \leq 5 \times 10^5\ \frac{kJ}{hr}$.

The safety-LMPC 2 for the process of Eq. (14) is designed to compute feasible control actions that drive the closed-loop state into the safety region quickly. Due to operation at the unstable steady-state, a Lyapunov-based controller of the form $h^T(x) = [h_1(x)\ h_2(x)]$ is constructed to estimate the stability region for the safety-LMPC 2. Also, a quadratic Lyapunov function $V(x) = x^T P x$ is used to construct the Lyapunov-based controller $h(x)$ where the weights of the P matrix were chosen to account for the different ranges of numerical values for each state. After extensive simulations, the P matrix was determined to be:

$$P = \begin{bmatrix} 850 & 18 \\ 18 & 3 \end{bmatrix}$$

To estimate the stability region Ω_ρ, the following feedback law (Sontag control law (Lin and Sontag (1991))) is utilized for the inlet concentration and heat rate (i.e., $u_i = h_i(x), i = 1, 2$):

$$h_i(x) = \begin{cases} -\dfrac{L_{\tilde{f}}V + \sqrt{L_{\tilde{f}}V^2 + L_{g_i}V^4}}{L_{g_i}V}, & \text{if } L_{g_i}V \neq 0 \\ 0, & \text{if } L_{g_i}V = 0 \end{cases} \tag{16}$$

where $L_{\tilde{f}}V$ and $L_{g_i}V$ are the Lie derivatives of the Lyapunov function $V(x)$ with respect to the vector fields $\tilde{f}(x)$ and $g_i(x)$ respectively. Both control laws are subject to input constraints. Under the control laws of Eq. (16) with input constraints, the stability region Ω_ρ is determined as a sufficiently large level set where the time-derivative of the Lyapunov function, $\dot{V}$, along the closed-loop state trajectories is negative. Fig. 3 shows the methodology for choosing the stability region. Specifically, the state-space region shown in Fig. 3 was discretized and the value of $\dot{V}$ along the closed-loop state trajectories of Eq. (14) under the control laws of Eq. (16) was evaluated at each discretized point. The grey region in Fig. 3 is the open neighborhood around the origin where $\dot{V}$ is negative. After these extensive simulations, ρ was found with value 2800.

The process was initiated from an initial condition that is relatively far from the steady-state (i.e., $x(t_0) = x_{int} = \left[-1.42192\ \frac{kmol}{m^3} 22\ K\right]$, and $V(x(t_0)) = 2044.42$) at time t_0. At this time, it is determined that the process state must move quickly into a region where the temperature deviates from the steady-state value by no more than 4.33 K (i.e., $\rho_{sp} = 50$) to avoid an unsafe operating condition. For this scenario, the abilities of the safety-LMPC 2 and classical LMPC formulations are compared to meet this safety goal with and without process disturbances. Both controllers drive the closed-loop state toward the steady-state, but the safety-LMPC design accomplishes this while controlling the rate at which the closed-loop state converges to the steady-state. The safety-LMPC 2 and the classical LMPC formulations considered are both implemented with a prediction horizon $N = 10$, a sampling period $\Delta = 0.01$ hr and an operating period of length $t_f = 1$ hr. The interior point solver Ipopt (Wächter and Biegler (2006)) was used to solve the optimization problems at each sampling time.

The safety-LMPC 2 formulation follows that in Eq. (9) with the objective function:

$$L(\tilde{x}, u, K_c) = \int_{t_k}^{t_{k+N}} \left[\tilde{x}(\tau)^T \tilde{x}(\tau) + u(\tau)^T u(\tau) + \frac{\left|\rho_{sp} - \tilde{\rho}(\tau)\right|^2}{h_c}\right] d\tau \tag{17}$$

The first two terms of Eq. (17) are the objective function of the classical LMPC where the weighting matrices are

$$Q = R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

This weighting was chosen because it is considered that the heat input u_2 is costly, and since the magnitude of u_2 can be much larger than the magnitude of x or u_1, the specified weighting matrices

Table 1
Parameter values.

$T_0 = 300$	K	$F = 5$	$\frac{m^3}{hr}$
$V = 1.0$	m^3	$E = 5 \times 10^4$	$\frac{kJ}{kmol}$
$k_0 = 8.46 \times 10^6$	$\frac{m^3}{kmolhr}$	$\Delta H = -1.15 \times 10^4$	$\frac{kJ}{kmol}$
$C_p = 0.231$	$\frac{kJ}{kgK}$	$R = 8.314$	$\frac{kJ}{kmolK}$
$\rho_L = 1000$	$\frac{kg}{m^3}$	$C_{As} = 2$	$\frac{kmol}{m^3}$
$T_s = 400$	K	$C_{A0s} = 4$	$\frac{kmol}{m^3}$
$Q_s = 0$	$\frac{kJ}{hr}$		

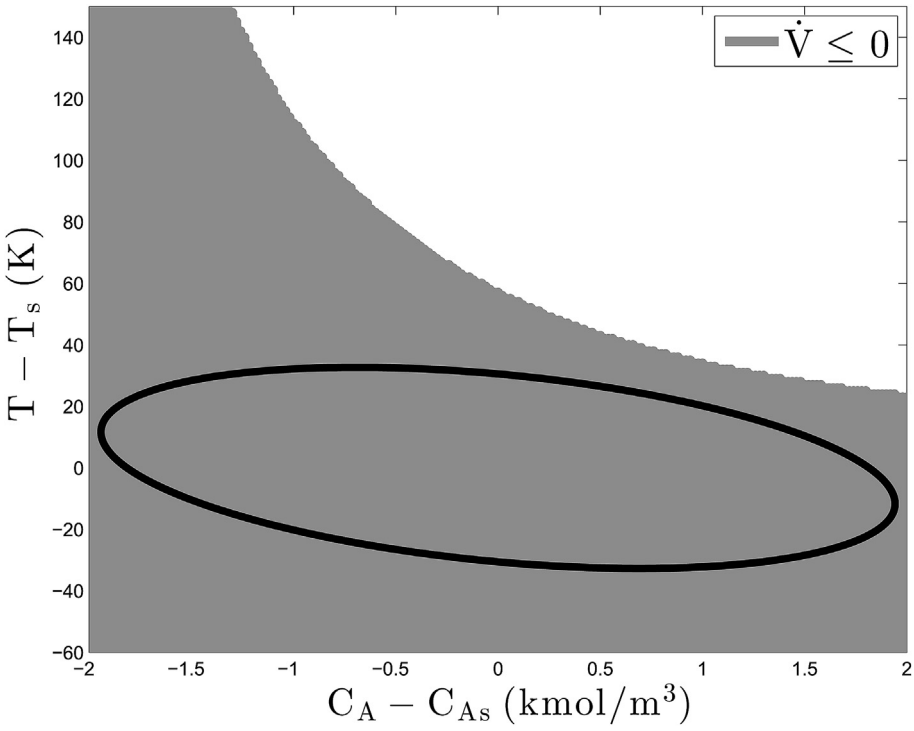

Fig. 3. The stability region (black ellipse) for the closed-loop CSTR under the explicit stabilizing controller $h(x)$ of Eq. (16).

prevent large values of u_2 from being requested and causing the value of Eq. (17) to become large. The third term in Eq. (17) is the safety penalty term where the squared Euclidean norm is chosen to penalize the deviation of the Lyapunov function value of the predicted closed-loop state $\tilde{\rho}(t)$ from the safety set-point ρ_{sp}. The safety penalty term is significantly penalized by a large weight $1/h_c$.

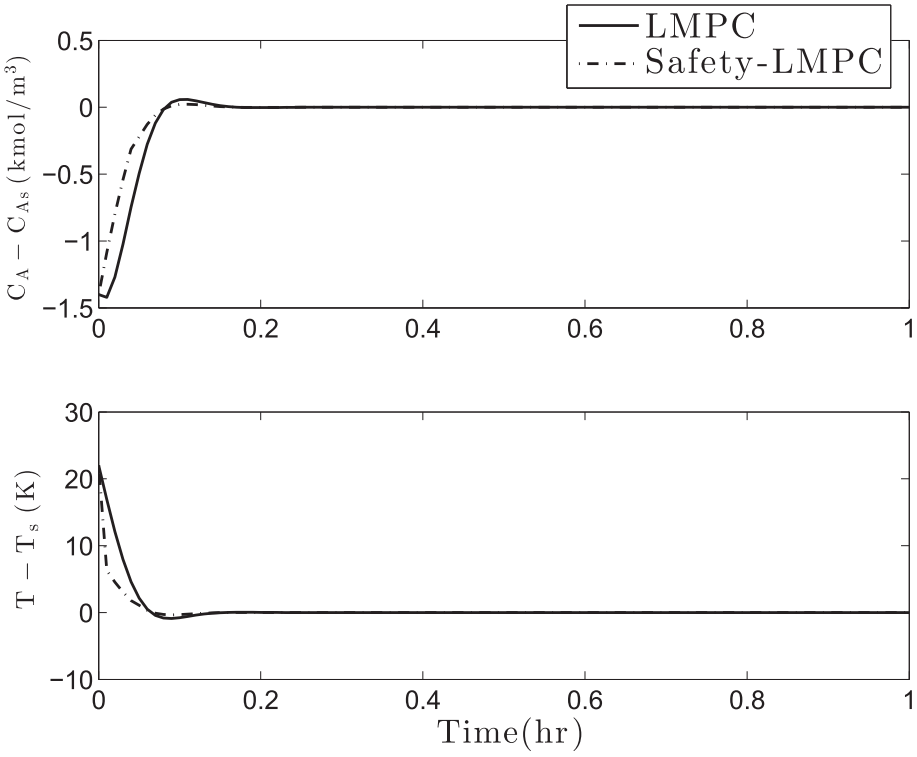

Fig. 4. The state profiles for the closed-loop CSTR under the classical LMPC design of Eq. (6) and under the safety-LMPC design of Eq. (9) for the initial condition $x_{int} = \left[-1.42192 \ \frac{kmol}{m^3} 22 \ K \right]$ without process disturbances.

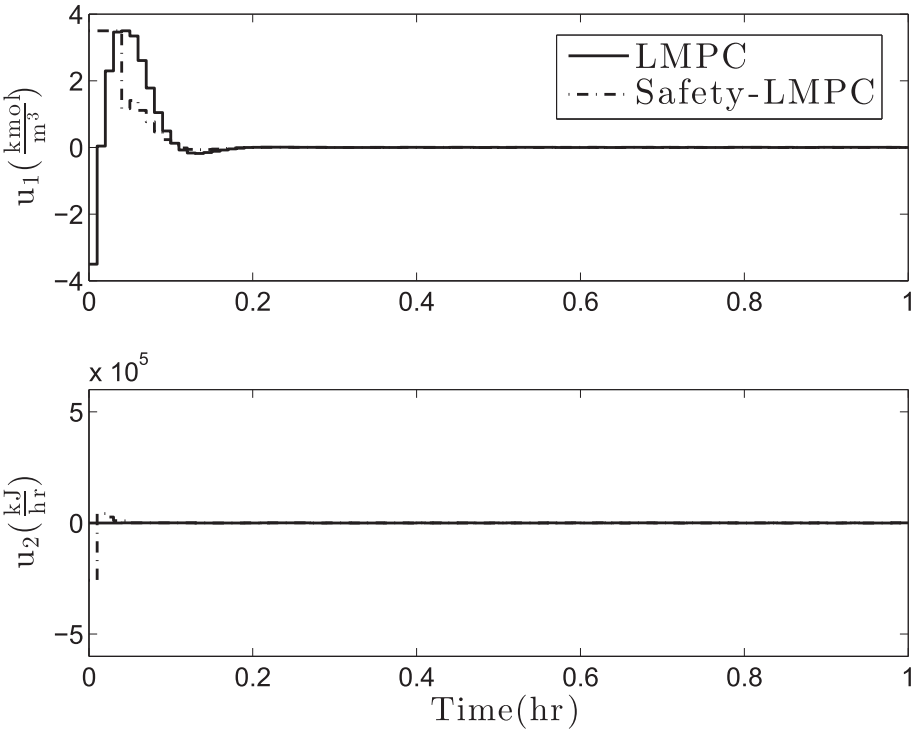

Fig. 5. Manipulated input profiles for the closed-loop CSTR under the classical LMPC design of Eq. (6) and under the safety-LMPC design of Eq. (9) for the initial condition $x_{int} = \left[-1.42192\ \frac{kmol}{m^3}\ 22\ K\right]$ without process disturbances.

Hence, the safety-LMPC 2 seeks to drive the closed-loop state into the safety region $\Omega_{\rho_{sp}}$ in a short time while using the minimum amount of energy u_2.

Figs. 4–5 show the closed-loop state trajectories and the manipulated input trajectories of the CSTR, initiated from x_{int}, under the safety-LMPC scheme and the classical LMPC scheme without process disturbances. From Fig. 4, the closed-loop state trajectory of the CSTR for the safety-LMPC 2 scheme reached the steady-state before that for the classical LMPC scheme. This is because the safety penalty term is highly penalized, which causes the closed-loop state to converge to the safety region more quickly than it does under the classical LMPC, and to then go to the steady-state. As shown in Fig. 5, the safety-LMPC 2 utilized a large amount of energy (i.e., $u_2 = -2.6 \times 10^5\ \frac{kJ}{hr}$) and the maximum amount of material (i.e., $u_1 = 3.5\ \frac{kmol}{m^3}$) in the first sampling period of the simulation to drive the closed-loop state into the safety region quickly due to the high weight on the safety penalty term. However, the classical LMPC used very little thermal energy (u_2) and less material (u_1) in the first sampling period of the simulation to minimize the value of the quadratic LMPC objective function.

Figs. 6–7 depict the Lyapunov function value of the closed-loop state, and the state-space profile for the closed-loop state, under both the safety-LMPC 2 and the classical LMPC without process disturbances. In Fig. 6, the closed-loop state under the safety-LMPC 2 entered the safety level set $\Omega_{\rho_{sp}}$ two sampling times before that under the classical LMPC. Fig. 7 demonstrates that the state-space profile for the closed-loop state under the classical LMPC drove the closed-loop state to the safety region even in the presence of disturbances due to the combination of the contractive constraint and the quadratic cost function of the classical LMPC. In addition, the safety-LMPC 2 scheme enhances the rate at which the closed-loop state approaches the safety region by the use of the safety penalty term and the safety-based constraints. After the closed-loop state trajectories under both schemes entered the safety region, they both reached the steady-state.

Figs. 8–9 show the corresponding state and manipulated input profiles starting from the same initial condition but under bounded process disturbances ($w^T = [w_1\ w_2]$ is the bounded disturbance vector corresponding to Gaussian white noise with variances $\sigma_1 = 1\ \frac{kmol}{m^3}$ and $\sigma_2 = 40\ K$) with $|w_1| \leq 1\ \frac{kmol}{m^3}$ and $|w_2| \leq 40\ K$. In the presence of disturbances, the safety-LMPC computes a value of u_1 that goes up to its allowable maximum value and u_2 reduces to its allowable minimum value in the first sampling period of the simulation to decrease the Lyapunov function value of the closed-loop state quickly, but the safety-LMPC eventually computes that both inputs should remain approximately at their steady-state values. Figs. 10 and 11 show the Lyapunov function value of the closed-loop state, and the state-space profile for the closed-loop state, under both the safety-LMPC 2 and the classical LMPC under bounded process disturbances. In the presence of uncertainty, the closed-loop state under the safety-LMPC 2 entered the safety region two sampling times before that under the classical LMPC (Fig. 10). Figs. 11 and 7 show that the closed-loop state trajectory under the safety-LMPC 2 chose a different path than the one for the classical LMPC, which led to an earlier entrance to the safety region by two sampling times in the presence and absence of uncertainty.

Remark 7. The proposed control-safety system integration methodology (safety-LMPC) is demonstrated in the context of the traditional continuous stirred tank reactor (CSTR) example. The CSTR example uses a generic A-> B reaction which corresponds to numerous industrial reactions. Generic reactions can be used to represent various industrial reactions including the production of propylene glycol from propylene oxide, which can be considered unsafe due to its exothermic nature and open-loop unstable steady-state (conceptually similar to the unstable steady-state analyzed for

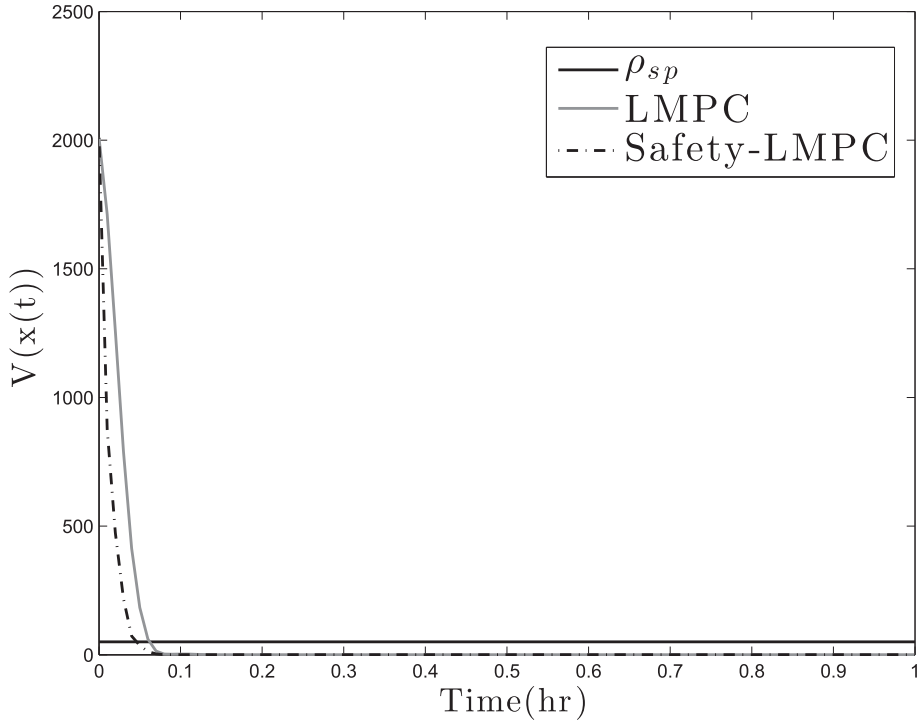

Fig. 6. The Lyapunov function value with time for the closed-loop CSTR under the classical LMPC design of Eq. (6) and under the safety-LMPC design of Eq. (9) for the initial condition $x_{int} = \left[-1.42192 \ \frac{kmol}{m^3} 22 \ K \right]$ without process disturbances. The safety set-point ρ_{sp} is also shown.

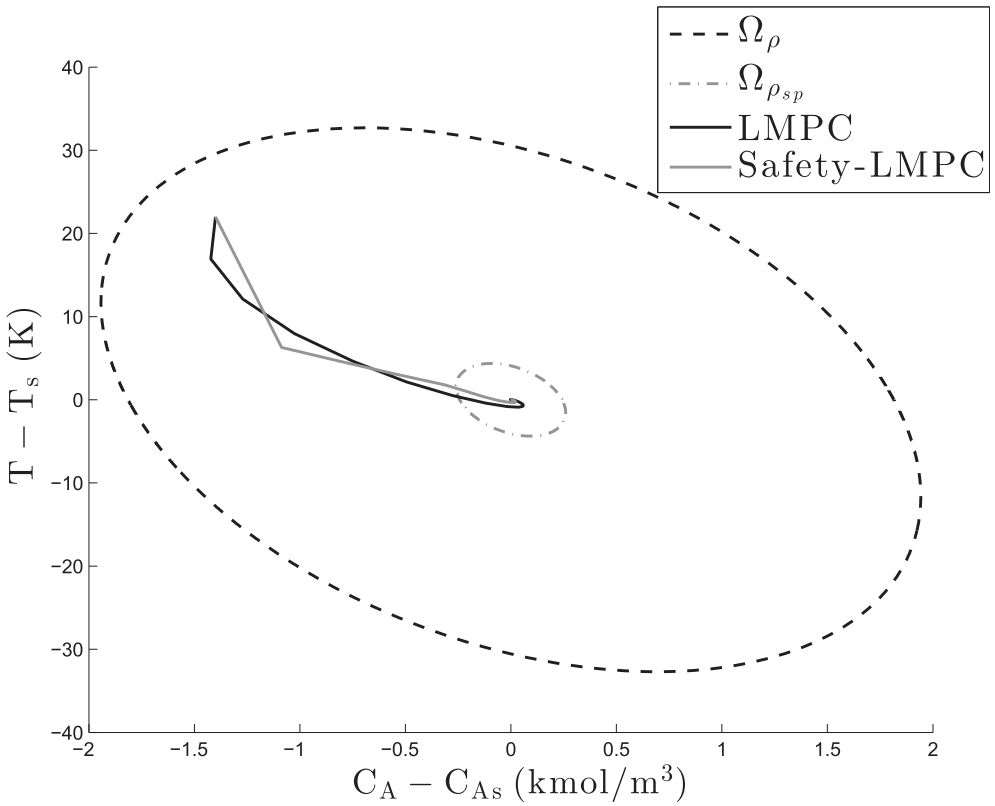

Fig. 7. The state-space profile for the closed-loop CSTR under the classical LMPC design of Eq. (6) and under the safety-LMPC design of Eq. (9) for the initial condition $x_{int} = \left[-1.42192 \ \frac{kmol}{m^3} 22 \ K \right]$ without process disturbances.

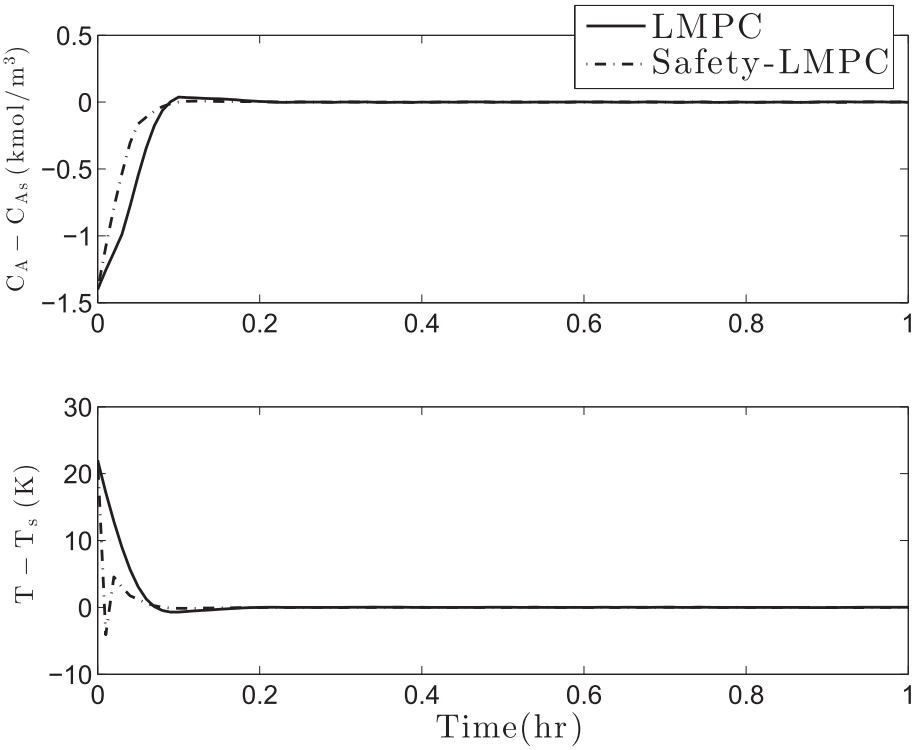

Fig. 8. The state profiles for the closed-loop CSTR under the classical LMPC design of Eq. (6) and under the safety-LMPC design of Eq. (9) for the initial condition $x_{int} = \left[-1.42192 \ \frac{kmol}{m^3} 22 \ K \right]$ with process disturbances.

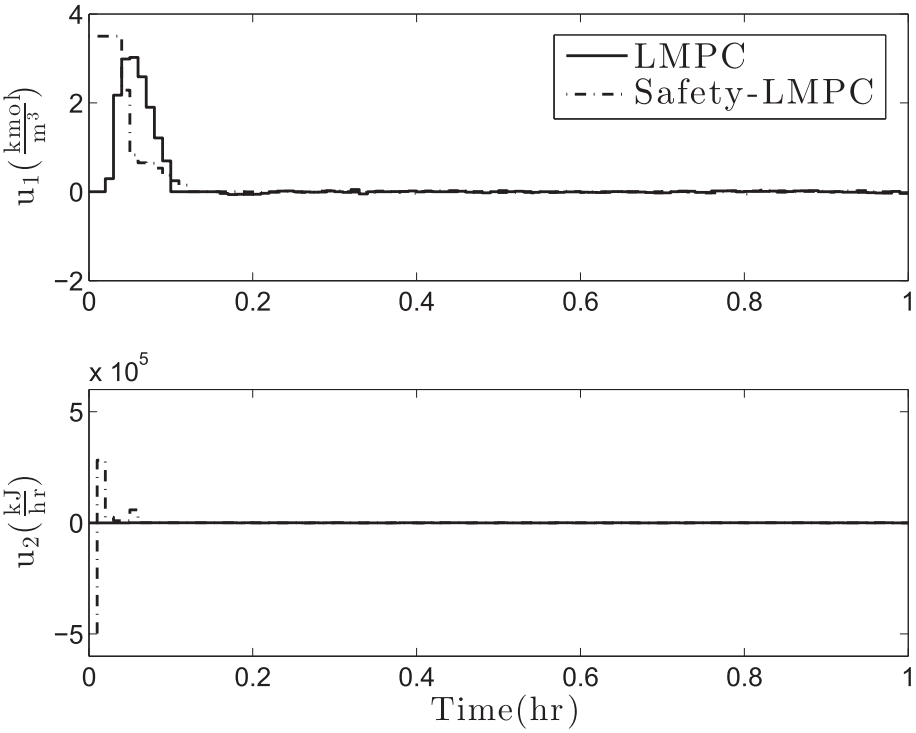

Fig. 9. Manipulated input profiles for the closed-loop CSTR under the classical LMPC design of Eq. (6) and under the safety-LMPC design of Eq. (9) for the initial condition $x_{int} = \left[-1.42192 \ \frac{kmol}{m^3} 22 \ K \right]$ with process disturbances.

the CSTR of Eq. (14)) from which open-loop deviations may result in the state moving toward a stable steady-state with a relatively high temperature. Therefore, incorporating safety-based constraints within the control system can reduce the number of alarms because the control system is now working to explicitly keep the closed-loop state in a safe region at all times.

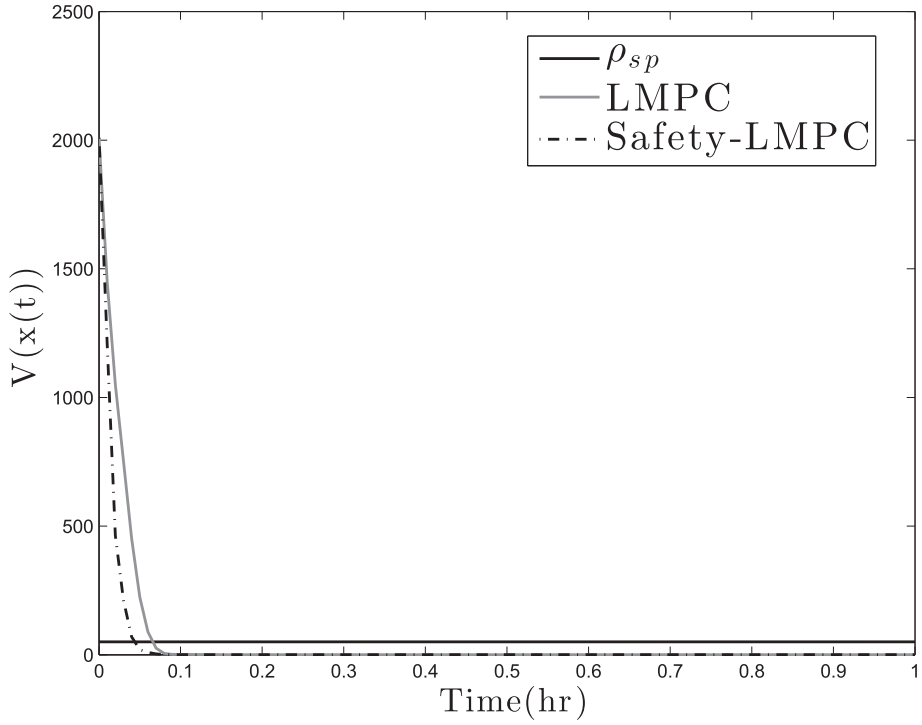

Fig. 10. The Lyapunov function value with time for the closed-loop CSTR under the classical LMPC design of Eq. (6) and under the safety-LMPC design of Eq. (9) for the initial condition $x_{int} = \left[-1.42192 \ \frac{kmol}{m^3} 22 \ K \right]$ with process disturbances. The safety set-point ρ_{sp} is also shown.

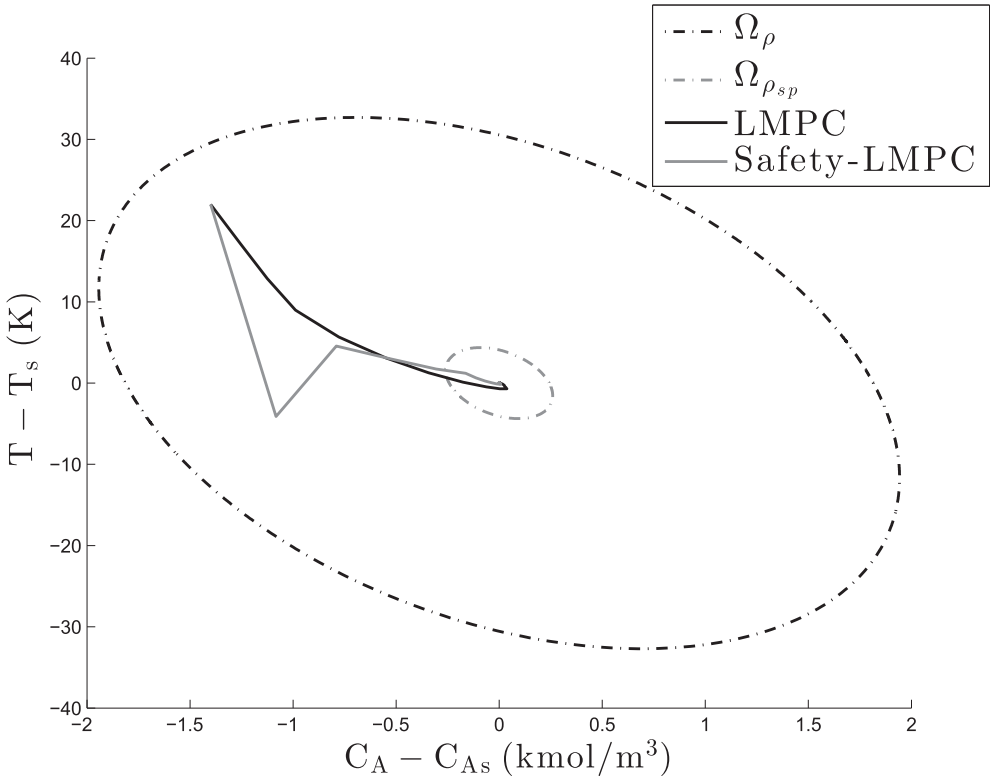

Fig. 11. The state-space profile for the closed-loop CSTR under the classical LMPC design of Eq. (6) and under the safety-LMPC design of Eq. (9) for the initial condition $x_{int} = \left[-1.42192 \ \frac{kmol}{m^3} 22 \ K \right]$ with process disturbances.

5. Conclusion

In this work, two LMPC schemes with safety-based constraints were presented to integrate feedback control and process functional safety within a unified framework. The motivation for the proposed safety-LMPC design was given, in particular that it can be formulated to drive the closed-loop state to a safe region of operation at a desired rate, which cannot easily be accomplished by tuning the weighting matrices in the quadratic objective function. The safety-LMPC's vary the upper bound on the level set of the Lyapunov function to achieve the improved rate of approach to the safety region, and they can also be modified to shift the region of operation from a level set around one steady-state to a level set around another. For a sufficiently small sampling period, a proof of recursive feasibility and closed-loop stability of a class of nonlinear systems under one of the safety-LMPC formulations in the presence of uncertainty was given. The safety advantage of the safety-LMPC paradigm over the classical LMPC paradigm was illustrated through a chemical process example. Nevertheless, the safety-based controller design was developed with a centralized model predictive control (MPC) structure; thus, computation time limitations within a sampling period may reduce the effectiveness of such a controller design for promoting process safety. An alternative MPC architecture that is intended to improve the computation time of the MPC algorithm is a distributed model predictive control (DMPC) architecture Christofides et al. (2011); Scattolini (2009). This MPC architecture has been investigated for computation time benefits since it can reduce the number of decision variables in each of the distributed optimization problems and may be able to terminate the optimization problems before the optimal solution is found while maintaining feasibility and closed-loop stability of the controller. A future work can be done to integrate a distributed Lyapunov-based model predictive control architecture formulated with safety-based constraints to decrease the computation time of the centralized safety-LMPC design.

Acknowledgements

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

References

Ahooyi, T.M., Soroush, M., Arbogast, J.E., Seider, W.D., Oktem, U.G., 2016. Model-predictive safety system for proactive detection of operation hazards. AIChE J. 62, 2024–2042.
Aswani, A., Gonzalez, H., Sastry, S.S., Tomlin, C., 2013. Provably safe and robust learning-based model predictive control. Automatica 49, 1216–1226.
Bahr, N.J., 2015. System Safety Engineering and Risk Assessment: A Practical Approach, second ed. CRC Press, Boca Raton, FL.
Carson, J.M., Açıkmeşe, B., Murray, R.M., MacMartin, D.G., 2013. A robust model predictive control algorithm augmented with a reactive safety mode. Automatica 49, 1251–1260.
Christofides, P.D., El-Farra, N.H., 2005. Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-delays. Springer-Verlag, Berlin, Germany.
Christofides, P.D., Liu, J., Muñoz de la Peña, D., 2011. Networked and Distributed Predictive Control: Methods and Nonlinear Process Network Applications. Springer Science & Business Media.
Crowl, D.A., Louvar, J.F., 2011. Chemical Process Safety: Fundamentals with Applications, third ed. Pearson Education, Upper Saddle River, NJ.
Dunjó, J., Fthenakis, V., Vílchez, J.A., Arnaldos, J., 2010. Hazard and operability (HAZOP) analysis. A literature review. J. Hazard. Mater. 173, 19–32.
El-Farra, N.H., Christofides, P.D., 2003. Bounded robust control of constrained multivariable nonlinear processes. Chem. Eng. Sci. 58, 3025–3047.
Gentile, M., Rogers, W.J., Mannan, M.S., 2003. Development of an inherent safety index based on fuzzy logic. AIChE J. 49, 959–968.
Heidarinejad, M., Liu, J., Christofides, P.D., 2012. Economic model predictive control of nonlinear process systems using Lyapunov techniques. AIChE J. 58, 855–870.
Heikkilä, A.M., Hurme, M., Järveläinen, M., 1996. Safety considerations in process synthesis. Comput. Chem. Eng. 20, S115–S120.
Kadri, S., Peters, G., VanOmmeren, J., Fegley, K., Dennehy, M., Mateo, A., 2014. So we all have been implementing process safety metrics-what next? Process Saf. Prog. 33, 172–178.
Khalil, H.K., 2002. Nonlinear Systems, third ed. Prentice Hall, Upper Saddle River, NJ.
Khan, F.I., Abbasi, S., 2000. Towards automation of HAZOP with a new tool EXPERTOP. Environ. Model. Softw. 15, 67–77.
Kletz, T., 2009. What Went Wrong? - Case Histories of Process Plant Disasters and How They Could Have Been Avoided, fifth ed. Elsevier, Burlington, Massachusetts.
Kletz, T.A., 1985. Inherently safer plants. Plant/Operations Prog. 4, 164–167.
Kletz, T.A., Amyotte, P., 2010. Process Plants: A Handbook for Inherently Safer Design, second ed. CRC Press, Boca Raton, FL.
Kokotović, P., Arcak, M., 2001. Constructive nonlinear control: a historical perspective. Automatica 37, 637–662.
Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42, 237–270.
Leveson, N.G., Stephanopoulos, G., 2014. A system-theoretic, control-inspired view and approach to process safety. AIChE J. 60, 2–14.
Lin, Y., Sontag, E.D., 1991. A universal formula for stabilization with bounded controls. Syst. Control Lett. 16, 393–397.
Mannan, M.S., Sachdeva, S., Chen, H., Reyes-Valdes, O., Liu, Y., Laboureur, D.M., 2015. Trends and challenges in process safety. AIChE J. 61, 3558–3569.
Marlin, T., 2012. Operability in Process Design: Achieving Safe, Profitable, and Robust Process Operations. McMaster University in Ontario, Canada.
Massera, J.L., 1956. Contributions to stability theory. Ann. Math. 64, 182–206.
Mayne, D.Q., Rawlings, J.B., Rao, C.V., Scokaert, P.O.M., 2000. Constrained model predictive control: stability and optimality. Automatica 36, 789–814.
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.
Moskowitz, I.H., Seider, W.D., Arbogast, J.E., Oktem, U.G., Pariyani, A., Soroush, M., 2016. Improved predictions of alarm and safety system performance through process and operator response-time modeling. AIChE J. 62, 3461–3472.
Muñoz de la Peña, D., Christofides, P.D., 2008. Lyapunov-based model predictive control of nonlinear systems subject to data losses. IEEE Trans. Automatic Control 53, 2076–2089.
Qin, S.J., Badgwell, T.A., 2003. A survey of industrial model predictive control technology. Control Eng. Pract. 11, 733–764.
Scattolini, R., 2009. Architectures for distributed and hierarchical model predictive control- A review. J. Process Control 19, 723–731.
Valipour, M., 2012. Comparison of surface irrigation simulation models: full hydrodynamic, zero inertia, kinematic wave. J. Agric. Sci. 4, 68–74.
Valipour, M., 2016. Optimization of neural networks for precipitation analysis in a humid region to detect drought and wet year alarms. Meteorol. Appl. 23, 91–100.
Valipour, M., Singh, V.P., 2016. Global Experiences on Wastewater Irrigation: Challenges and Prospects. In: Maheshwari, B., Singh, V.P., Thoradeniya, B. (Eds.), Balanced Urban Development: Options and Strategies for Liveable Cities. Springer Open, pp. 289–327.
Venkatasubramanian, V., 2011. Systemic failures: challenges and opportunities in risk management in complex systems. AIChE J. 57, 2–9.
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.
Whiteley, J.R., 2006. Potential use of advanced process control for safety purposes during attack of a process plant. J. Hazard. Mater. 130, 42–47.
Yannopoulos, S.I., Lyberatos, G., Theodossiou, N., Li, W., Valipour, M., Tamburrino, A., Angelakis, A.N., 2015. Evolution of water lifting devices (pumps) over the centuries worldwide. Water 7, 5031–5060.