A Feedback Control Framework for Safe and Economically-Optimal Operation of Nonlinear Processes

Fahad Albalawi
Dept. of Electrical Engineering, University of California, Los Angeles, CA 90095

Anas Alanqar and Helen Durand
Dept. of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095

Panagiotis D. Christofides
Dept. of Chemical and Biomolecular Engineering and Dept. of Electrical Engineering,
University of California, Los Angeles, CA 90095

DOI 10.1002/aic.15222
Published online March 27, 2016 in Wiley Online Library (wileyonlinelibrary.com)

Maintaining safe operation of chemical processes and meeting environmental constraints are issues of paramount importance in the area of process systems and control engineering, and are ideally achieved while maximizing economic profit. It has long been argued that process safety is fundamentally a process control problem, yet few research efforts have been directed toward integrating the rather disparate domains of process safety and process control. Economic model predictive control (EMPC) has attracted significant attention recently due to its ability to optimize process operation accounting directly for process economics considerations. However, there is very limited work on the problem of integrating safety considerations in EMPC to ensure simultaneous safe operation and maximization of process profit. Motivated by the above considerations, this work develops three EMPC schemes that adjust in real-time the size of the safety sets in which the process state should reside to ensure safe process operation and feedback control of the process state while optimizing economics via time-varying process operation. Recursive feasibility and closed-loop stability are established for a sufficiently small EMPC sampling period. The proposed schemes, which effectively integrate feedback control, process economics, and safety considerations, are demonstrated with a chemical process example. © 2016 American Institute of Chemical Engineers *AIChE J*, 62: 2391–2409, 2016

Keywords: economic model predictive control, process safety, process control, process optimization

Introduction

Safe operation of chemical processes plays a vital role in the chemical and petrochemical industry. It has been reported that the 20 accidents that caused the largest property damage losses in the hydrocarbon industry from 1972 to 2011 cost $14.6 billion in such losses.[1] Clearly, process safety has a great impact on economic profitability, stable production, environmental damage, and human injury.[2] As technological advances increase the economic profitability of chemical processes, the complexity of ensuring safe operation increases.[3] A good strategy to handle such complex processes is to introduce methods that can predict and control the interactions between the components of the complex processes.[4] In industry, the safety of a chemical process is often evaluated through methods based on accident causation and statistics such as hazards and operability studies, fault trees, event trees, what-if scenarios, and worst-case scenarios, which are performed by engineers, chemists, operators, industrial hygienists, and other experts to suit the complexity of the process considered. These studies often result in a qualitative or quantitative description of damage that may result from an accident (including life losses, capital equipment loss, and damage to the environment) which is evaluated to determine whether it is within an acceptable level of risk.[5] Process safety is also evaluated through layers of protection analysis, which is conducted during or after the process design stage to determine whether there are sufficient barriers to accidents (e.g., process control, alarms, and containment areas) to ensure safe operation of the process considered.[5]

In the chemical processing industry, the most important approach for promoting process safety, which is designing a process to be inherently safe, is performed by engineers at the design phase. Inherent safety refers to the innate safeness of a chemical process based on the chemical and physical properties, phenomena, and dynamics of the process, and can be adjusted by, for example, choosing a different catalyst, reaction pathway, reactant, or operating pressure. To assess the inherent safety of a chemical plant, methods incorporating Boolean mathematics[6] and fuzzy logic theory[7] can be used. The construction of an inherently safe process requires the selection of processing conditions that eliminate or reduce hazards, rather than developing add-on protective layers and systems such as process control systems. New technology

Correspondence concerning this article should be addressed to P. D. Christofides at pdc@seas.ucla.edu.

enables the construction of more inherently safe processes with lower operating costs, increased profitability, and increased reliability.[5]

The second most important safety approach for chemical plants is the design of an effective process control system.[5] A control system is only effective, however, when the control software is well-designed and the operator is trained to take appropriate action in unsafe rare events.[8,9] However, from a safety perspective, the most common industrial control strategy currently in use, the traditional single-input/single-output feedback control loop (e.g., PID controllers), lacks many of the capabilities that would be desired from a control system designed to ensure process safety. The primary drawback of these types of controllers from a safety perspective is that they are unable to account for actuator constraints, state constraints expressing process operation in a safe region, and multi-variable interactions for complex processes.[10] In addition, such a simple control structure is less adaptable to federal and environmental regulation changes.[5]

Alternatively, advanced control methodologies can be integrated with safety considerations because they are able to deal with multi-variable interactions using the process model and at the same time can compute control actions that account for actuator constraints.[3,11] Model predictive control (MPC), for example, an advanced control technique that takes into account multi-variable interactions and actuator limitations, can be used for improved control and safety.[3,10,12] MPC is characterized by the use of optimization and a dynamic process model to compute optimal control actions that typically drive the state of the process to a desired steady-state.[13–15] 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[16] and a two-mode MPC with a standard mode and a reactive safety mode was designed to account for unexpected state-constraint changes.[17] Recently, a form of MPC termed economic model predictive control (EMPC) that optimizes process operation through dynamic operation rather than by driving the process to a steady-state, has gained attention.[18–21] The shift that EMPC represents from a steady-state operation paradigm to a time-varying operation paradigm does not come without risk. Regardless of the degree of performance benefit that may be realized by applying EMPC, maintaining safe operation of process systems is of the highest priority. It has been argued, however, that safety can be used as a constraint in control systems to allow a control system to simultaneously address process control and process safety.[3] However, mathematically formalizing this vision of integrating safety and process control is an open and challenging area as new safety metrics, process monitoring methodologies, and control schemes that incorporate safety as a constraint need to be introduced. Several works have shown that EMPC is capable of addressing safety in a proactive sense, in that it is able to account for preventive maintenance of sensors[22] and of actuators[23] to prevent faults that could lead to unsafe conditions. However, despite the fact that EMPC provides a natural framework for integrating operational safety considerations and feedback control because it is a unique predictive control technique that uses a general cost function in its formulation which may be formulated to incorporate both economic and safety considerations, no treatment of safety integrated with EMPC in a general sense has been performed.

In this work, we develop three Lyapunov-based EMPC (LEMPC) schemes with safety-based constraints based on a Lyapunov function for the closed-loop system termed safety-LEMPC that guarantee safe operation of a class of nonlinear process systems by varying the allowable region of operation. Specifically, the safety-LEMPC's drive the process state from a normal region of operation to a subset of this region (termed the safety region) by activating safety-based constraints at a certain time (the switching time). In scheme 1, the safety-LEMPC drives the closed-loop state trajectory of the process into a safe region of operation using a contractive constraint, starting at the switching time, that ensures that the closed-loop state enters the safety region at least as quickly as it would under an explicit Lyapunov-based controller. However, the contractive constraint alone may not guarantee that the state will be driven quickly to the safety region after the switching time. Therefore, in scheme 2 the safety-LEMPC exploits a longer prediction horizon and a region constraint to drive the closed-loop state to the safety region by the switching time. In an EMPC optimization framework, a long prediction horizon implies a large number of decision variables which may require a long computation time.

To overcome the drawbacks of the first two schemes, scheme 3 introduces two different optimization formulations that incorporate time-varying safety-based constraints to efficiently move the closed-loop state from the normal region of operation to the safety region. In the first formulation of scheme 3, the safety-LEMPC utilizes slack variables and a penalty term in the objective to increase the rate at which the closed-loop state enters the safety region. The second formulation of scheme 3, termed dynamic safety level set-LEMPC (DSLS-LEMPC), is a safety-LEMPC design that dynamically controls the upper bound on the level set of the Lyapunov function of the closed-loop state. Specifically, the DSLS-LEMPC includes a first-order ordinary differential equation that governs the rate of decrease of the upper bound on the level set of the Lyapunov function in addition to a penalty term in the objective function to enhance the rate at which the closed-loop state goes to the safety region. Suitable constraints for the safety-LEMPC's are developed that ensure that the closed-loop system state is bounded in a pre-defined safety region and is ultimately bounded in a compact set containing the origin. Recursive feasibility and guaranteed closed-loop stability for a nonlinear process under the safety-LEMPC schemes are proven for a sufficiently small sampling period. Through a chemical process example, the three proposed safety-LEMPC schemes, which effectively integrate feedback control, process economics, and safety considerations, are demonstrated.

Preliminaries

Notation

The L^2 norm of a vector is denoted by the operator $|\cdot|$. The transpose of a vector x is represented by the symbol x^T. 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 functions with period $\Delta \geq 0$. A diagonal matrix which has the components of a vector s as its diagonal elements is denoted by the symbol $\mathrm{diag}(s)$. Set subtraction is denoted by the operator "/," that is, $A/B := \{x \in R^n : x \in A, x \notin B\}$. A function

$\alpha(\cdot) : [0, a) \to [0, \infty)$ belongs to class $\mathcal{K}$ (i.e., $\alpha \in \mathcal{K}$) if it is strictly increasing and continuous, and $\alpha(0)=0$.

Class of nonlinear process systems

The class of nonlinear process systems considered is as follows:

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

where $x(t) \in R^n$ is the state vector of the system, and $u(t) \in R^m$ and $w(t) \in R^w$ are the control (manipulated) input vector and the disturbance vector, respectively. The admissible input values are restricted to m nonempty convex sets $U_i \subseteq R$, $i=1, \ldots, m$, where $U_i := \{u_i \in R : u_i^{\min} \leq u_i \leq u_i^{\max}\}$, and $u_i^{\max}$ and $u_i^{\min}$, $i=1, \ldots, m$, are the magnitudes of the input constraints which result from the physical constraints on the control actuators. We assume that f is a locally Lipschitz vector function of its arguments and that the state of the system of Eq. 1 is synchronously sampled at time instances $t_k=t_0+k\Delta,\ k=0, 1, \ldots$, where Δ is the sampling period and t_0 is the initial time. The disturbance $w(t)$ is bounded within the set $W := \{w \in R^w : |w| \leq \theta, \theta > 0\}$ (i.e., $w(t) \in W$). We assume that the origin is an equilibrium point of the unforced nominal system which implies that $f(0, 0, 0)=0$.

Stabilizability assumption

We consider nonlinear systems that are stabilizable in the sense that there exists 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. We further assume the existence[24,25] of a sufficiently smooth Lyapunov function $V(x)$ for the nominal closed-loop system and class $\mathcal{K}$ functions $\alpha_i(\cdot)$, $i=1, 2, 3, 4$ such that the following inequalities hold:

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

for all $x \in D \subseteq R^n$ where D is an open neighborhood of the origin. We define a level set of the Lyapunov function within which $\dot{V}$ is negative as the stability region Ω_ρ of the process of Eq. 1 under $h(x)$ (where $\Omega_\rho \subseteq D$; see, for example,[26–29] for results on the design of stabilizing control laws).

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:

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

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

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

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

Lyapunov-Based EMPC

Lyapunov-based economic model predictive control (LEMPC) is an optimization-based control strategy implemented in a receding horizon fashion that utilizes the Lyapunov-based controller $h(x)$ as follows[20]:

$$\min_{u \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau))\ d\tau \tag{6a}$$

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

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

$$u_i(t) \in U_i,\ \ i=1, \ldots, m,\ \ \forall\ t \in [t_k, t_{k+N}) \tag{6d}$$

$$\begin{gathered} V(\tilde{x}(t)) \leq \rho_e,\ \ \forall\ t \in [t_k, t_{k+N}) \\ \text{if}\ \ x(t_k) \in \Omega_{\rho_e} \end{gathered} \tag{6e}$$

$$\begin{gathered} \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \\ \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0) \\ \text{if}\ \ x(t_k) \notin \Omega_{\rho_e} \end{gathered} \tag{6f}$$

where the piecewise constant input trajectory $u(t)$ is the decision variable of the optimization problem defined over the prediction horizon with N sampling periods of length Δ, and the predicted state trajectory is denoted by $\tilde{x}(t)$. The nominal model of Eq. 1 is used to predict the evolution of the system over the prediction horizon (Eq. 6b) where the initial condition of the dynamic system is obtained through a state measurement at the current sampling time t_k (Eq. 6c). Equation 6a is the objective function of the LEMPC design, where the stage cost $L_e(\tilde{x}, u)$ reflects the process economics of the class of nonlinear systems of Eq. 1. The constraint of Eq. 6d restricts the control actions $u(t)$ to be within the admissible set over the prediction horizon.

In Mode 1 (Eq. 6e), the LEMPC optimizes the economic cost function of Eq. 6a in a time-varying fashion when the state measurement of Eq. 6c is within the region Ω_{ρ_e}, which is a subset of Ω_ρ. This subset Ω_{ρ_e} is selected to make the stability region Ω_ρ a forward invariant set for the closed-loop process under LEMPC in the presence of disturbances (i.e., if the process is initialized within Ω_ρ, the closed-loop state is maintained within Ω_ρ for all time). In Mode 2 (Eq. 6f), which is activated when $x(t_k) \in \Omega_\rho/\Omega_{\rho_e}$, the contractive constraint utilizes the explicit stabilizing controller $h(x)$ to drive the closed-loop state back into Ω_{ρ_e} by computing control actions that decrease the value of the Lyapunov function at least as much as the decrease given by the stabilizing controller.

Safety-LEMPC Structure

The major contribution of this work is the development of control schemes that address safety in a control design framework through the incorporation of constraints based on safety considerations. In this work, three LEMPC schemes (termed safety-LEMPC schemes) are presented that couple the ability of LEMPC to optimize profit with its ability to handle safety considerations by accounting for multivariable interactions, constraints, and a general objective function. These safety-LEMPC schemes add various safety-based constraints to the standard formulation of LEMPC in Eq. 6 so that safety is enforced as a constraint of operation, which allows for economic optimization to be pursued among all solutions to the optimization problem that satisfy the safety criteria.

In this section, we provide descriptions of the three proposed safety-LEMPC schemes with safety-based constraints. Specifically, a detailed description of the implementation strategy for the safety-LEMPC schemes, the formulations of the schemes, and a chemical process example for each scheme are presented. Moreover, provable stability and feasibility properties of the safety-LEMPC's are given.

Implementation strategy

The classical LEMPC design[20] dictates time-varying operation to maximize the profit while maintaining the closed-loop state of the process in the stability region Ω_ρ. The stability region Ω_ρ may be estimated as the largest level set of the Lyapunov function where the time-derivative of the Lyapunov function is negative along the closed-loop state trajectories of the nominal system of Eq. 1 under $h(x)$ for all points in the level set. However, there may be regions in Ω_ρ within which it becomes unsafe to operate the process for some period of time due to disturbances (e.g., significant disturbances in the concentration of the feed stream, disturbances in ambient temperature, actuator problems such as a sticking valve). In such scenarios, it is necessary to change the allowable region of operation in real-time from Ω_ρ to a smaller level set of the Lyapunov function where safe process operation is achieved to maintain the closed-loop state within a safe region of operation. In this work, we present three LEMPC schemes with safety-based constraints called safety-LEMPC that can update the level set of the Lyapunov function online to tackle the following two tasks:

Task 1: Driving the closed-loop state of the process of Eq. 1 under the safety-LEMPC into a safe region of operation.

Task 2: Maintaining the closed-loop state of the process of Eq. 1 under the safety-LEMPC in this safe region of operation.

Figure 1 depicts the implementation strategy of the safety-LEMPC paradigm. As shown in Figure 1, a safety logic unit determines an appropriate level set for safe process operation by using data on the probability of potential failures of process equipment or software components, measurement feedback of the process state and the estimated future process state trajectory. If it is determined that an equipment or software failure or other unsafe scenario is likely, the safety logic unit communicates the most profitable safety set-point ρ_{sp} to the safety-LEMPC to cause it to drive the closed-loop state to a safe region of operation termed the safety region $\Omega_{\rho_{sp}}$ and maintain the process operation there. The control actions computed by the safety-LEMPC will be applied to the plant in a sample-and-hold fashion, and the measured state will be fed back to both the safety-LEMPC for controller robustness and the safety logic unit so that the safety level set will be re-evaluated if necessary.

Remark 1. If no process faults or unsafe conditions are predicted by the safety logic unit, ρ_{sp} will be chosen as the largest level set in the stability region where closed-loop stability in the presence of uncertainty is guaranteed to maximize the economic measure of the safety-LEMPC.

Remark 2. In Figure 1, the safety logic unit receives the state measurement from the plant regularly; however, the safety logic unit may communicate a new value of ρ_{sp} to the safety-LEMPC less frequently.

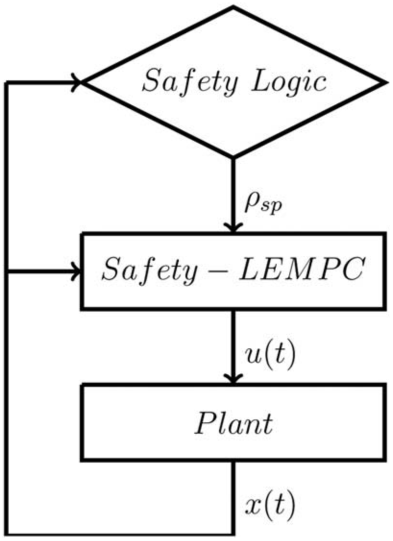

Figure 1. The implementation strategy of the safety-LEMPC paradigm.

Remark 3. The safety-LEMPC schemes that will be presented are not intended to sacrifice process safety for economic performance. Rather, the three schemes to be presented are intended for different purposes (e.g., one scheme may be better suited for processes where rapid and safety-critical switches of the region of operation are necessary, while another may be better suited for processes where the transition to a new region of operation can be slower without negative consequences, such as a process for which high temperature operation is acceptable for a small period of time although it is safer to move it to a region where the temperature is lower after this time to avoid, for example, material weakening). A control engineer would choose the desired scheme and tune any parameters of the desired scheme in a manner that provides acceptable control and safety for a given process. Advantages and disadvantages of the three safety-LEMPC's will be presented in the discussion of each below to elucidate some of the factors that should be considered when selecting a safety-LEMPC scheme. The safety-LEMPC system is not intended to replace traditional process safety systems. It is, however, intended to be used in place of other EMPC schemes that may be used to control a process to augment the traditional safety systems that would also be used to provide an additional means of increasing process safety.

Scheme 1: LEMPC Using Level-Set Switching

As noted in the "Implementation strategy" section, the two tasks of the safety-LEMPC are to shift the region of operation to a safer zone and to maintain the closed-loop states within this safer zone. The first considered scheme tackles these tasks by applying the standard LEMPC scheme of Eq. 6 (with the Mode 1 and Mode 2 constraints defined with respect to Ω_{ρ_e}) until a switching time t_1 at which time it is desired that the closed-loop state moves toward a lower level set $\Omega_{\rho_{sp}}$ (the safety region) that is within the stability region. At this time, the level set that determines whether the Mode 1 or Mode 2 constraint should be used is re-defined in terms of $\Omega_{\bar{\rho}_{sp}}$, which is a subset of $\Omega_{\rho_{sp}}$ defined to make $\Omega_{\rho_{sp}}$ an invariant set under the safety-LEMPC in the presence of disturbances/uncertainty once the state enters $\Omega_{\rho_{sp}}$ (i.e., the relationship between $\Omega_{\bar{\rho}_{sp}}$

and $\Omega_{\rho_{sp}}$ is similar to that between Ω_{ρ_e} and Ω_ρ). Thus, the effect of this safety-LEMPC scheme is to enforce the Mode 2 contractive constraint starting from the state $x(t_1) \in \Omega_\rho$ until the closed-loop state enters $\Omega_{\bar{\rho}_{sp}}$, so that the rate at which the state approaches the safety region is no worse than the rate at which the state would approach $\Omega_{\bar{\rho}_{sp}}$ under the Lyapunov-based controller $h(x)$. Due to the closed-loop stability property of the explicit stabilizing controller $h(x)$, this scheme is guaranteed to drive the closed-loop state to the lower level set $\Omega_{\bar{\rho}_{sp}}$ in the presence of uncertainty.[30] Once the state enters $\Omega_{\bar{\rho}_{sp}}$, the safety-LEMPC dictates time-varying operation to maximize the profit while the measured state remains within $\Omega_{\bar{\rho}_{sp}}$, but uses the contractive constraint when $x(t_k) \in \Omega_{\rho_{sp}}/\Omega_{\bar{\rho}_{sp}}$ to ensure process operation is maintained within the safety region $\Omega_{\rho_{sp}}$ in the presence of disturbances/uncertainty (the proof of this will be clarified in the section "Feasibility and stability analysis").

The formulation of this control strategy is presented in the following optimization problem:

$$\max_{u \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau)) \, d\tau \tag{7a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0), \ \tilde{x}(t_k) = x(t_k) \tag{7b}$$

$$u_i(t) \in U_i, \ i = 1, \ldots, m, \ \forall \ t \in [t_k, t_{k+N}) \tag{7c}$$

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

$$\hat{\rho} = \rho_e, \quad \text{if } x(t_k) \in \Omega_{\rho_e} \text{ and } t_k < t_1 \tag{7d}$$

$$\hat{\rho} = \bar{\rho}_{sp}, \quad \text{if } x(t_k) \in \Omega_{\bar{\rho}_{sp}} \text{ and } t_k \geq t_1$$

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

$$\text{if } x(t_k) \notin \Omega_{\rho_e} \text{ and } t_k < t_1 \text{ or if } x(t_k) \notin \Omega_{\bar{\rho}_{sp}} \text{ and } t_k \geq t_1 \tag{7e}$$

Remark 4. Although this scheme is guaranteed to drive the closed-loop state of Eq. 1 to the desired safety region, it is not guaranteed to do so in a fast or proactive fashion (i.e., there is no adjustable parameter in this scheme that can be changed to modify the time that it takes to drive the closed-loop state into $\Omega_{\rho_{sp}}$ after t_1). Often, safety constraints are required to be satisfied in a measurable amount of time; as a result, this scheme may present an issue for practical implementation in certain scenarios. However, it is also possible to perform extensive closed-loop simulations of the process under $h(x)$ in the presence of bounded disturbances/uncertainty for initial values $x(t_1) \in \Omega_\rho$ throughout the stability region before implementing this safety-LEMPC scheme. From these simulations, it is possible to determine the worst-case rate of approach to a variety of possible safety level sets to determine whether the rate of transition from Ω_ρ to $\Omega_{\rho_{sp}}$ would be acceptable for a given process.

Remark 5. The economic optimality of a feasible control action plays a significant role in the safety-LEMPC's selection of control actions in this scheme. Because the constraint of Eq. 7e only requires that the state move toward $\Omega_{\rho_{sp}}$ at least as quickly as it would under $h(x)$, the LEMPC will choose a control action that maximizes profit during this approach since that is the required objective in this case, and thus it will not choose a different control action that may cause the closed-loop state to more quickly approach the safety region but with less economic benefit during this approach. However, the emphasis of this scheme on economics during the approach to the safety region as opposed to the speed with which the approach to the safety region occurs is an important consideration when determining whether this controller is the best safety-LEMPC to apply for a given process. In circumstances where the known Lyapunov-based controller does not provide a satisfactory rate of approach of the process state to the safety region, this more economically-focused safety-LEMPC may be inadequate to ensure that the safety region is approached in the timeframes that may be desired. However, for processes for which the worst-case rate of approach to a safety region under $h(x)$ is considered to be acceptable, the economic focus of the LEMPC during the transition to the safety region (the transition period) may be economically beneficial while still ensuring that all safety requirements are met.

Table 1. Parameter Values

$T_0 = 300$	K	$F = 5$	$\frac{m^3}{hr}$
$V = 1.0$	m^3	$E = 5 \times 10^4$	$\frac{kJ}{kmol}$
$k_0 = 8.46 \times 10^6$	$\frac{m^3}{kmolhr}$	$\Delta H = -1.15 \times 10^4$	$\frac{kJ}{kmol}$
$C_p = 0.231$	$\frac{kJ}{kgK}$	$R = 8.314$	$\frac{kJ}{kmolK}$
$\rho_L = 1000$	$\frac{kg}{m^3}$	$C_{As1} = 1.2$	$\frac{kmol}{m^3}$
$T_{s1} = 438$	K	$C_{As2} = 2$	$\frac{kmol}{m^3}$
$T_{s2} = 400$	K	$C_{A0s} = 4$	$\frac{kmol}{m^3}$
$Q_s = 0$	$\frac{kJ}{hr}$		

Scheme 1: application to a chemical process example

In this section, we demonstrate scheme 1 of the safety-LEMPC using a chemical process example. Because this chemical process example will also be used for the demonstration of the other safety-LEMPC schemes developed in this work, we will begin with a general statement of the control problem that will be used in the demonstration of all three schemes, and will then focus on the parameters chosen specifically to demonstrate scheme 1, and the closed-loop results for the process under scheme 1.

The chemical process considered is a well-mixed, non-isothermal continuously stirred tank reactor (CSTR) within which a reactant A is transformed to a product B through the exothermic, irreversible second-order reaction $A \rightarrow B$.[31] The CSTR is fed with pure A at flow rate F, concentration C_{A0}, and temperature T_0, and it is cooled and heated at heat rate Q by a jacket. The concentration of A (C_A) and temperature T in the reactor are modeled using mass and energy balances with standard modeling assumptions as follows:

$$\frac{dC_A}{dt} = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{RT}} C_A^2 \tag{8a}$$

$$\frac{dT}{dt} = \frac{F}{V}(T_0 - T) + \frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{RT}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{8b}$$

where ΔH, k_0, E, and R are the enthalpy of reaction, pre-exponential constant, activation energy, and ideal gas constant. The reactor volume V, heat capacity C_p, and fluid density ρ_L within the reactor are assumed constant. The values of these parameters are given in Table 1.

The two manipulated inputs of the CSTR are the inlet concentration C_{A0} and the heat input/removal rate Q. These manipulated inputs are bounded as follows: $0.5 \leq C_{A0} \leq 7.5\ kmol/m^3$ and $|Q| \leq 5\times10^5\ kJ/hr$.

In the operating region of interest, the process model of Eq. 1 has one stable steady-state ($[C_{As1}\ T_{s1}] = [1.2\ \frac{kmol}{m^3}\ 438\ K]$) and one unstable steady-state ($[C_{As2}\ T_{s2}] = [2\ \frac{kmol}{m^3}\ 400\ K]$) corresponding to the steady-state input $[C_{A0s}\ Q_s]$ given in Table 1 (steady-states outside the operating region of interest are not considered). The dynamic model of Eq. 8 is a member of the class of nonlinear systems of Eq. 1 with $w(t) \equiv 0$, where $x = [C_A - C_{As}\ T - T_s]^T$ is the state vector ($C_{As} = C_{As1}$ or C_{As2}, and $T_s = T_{s1}$ or T_{s2}) and $u = [C_{A0} - C_{A0s}\ Q - Q_s]^T$ is the input vector. In particular, it is an input-affine nonlinear system with the form:

$$\dot{x}(t) = \tilde{f}(x(t)) + g(x(t))u(t) \tag{9}$$

The explicit Euler method with an integration time step of $h_c = 10^{-5}\ hr$ was applied to numerically simulate the dynamic model of Eq. 8.

The control objective is to maximize the profit of the CSTR process of Eq. 8 while driving the closed-loop state trajectories to a safe region of operation when required by controlling the process using a safety-LEMPC scheme. To maximize the profit, the objective function of the safety-LEMPC optimizes the following stage cost, which represents the production rate of B:

$$L_e(x,u) = k_0 e^{-\frac{E}{RT}} C_A^2 \tag{10}$$

The process and basic design parameters of the safety-LEMPC presented above are now used in the demonstration of scheme 1 (and, as noted, that same problem formulation will be used in the demonstration of the other safety-LEMPC schemes developed in this work). In the demonstration of scheme 1 using this chemical process example, the process is operated around the stable steady-state of the CSTR with steady-state input values $[C_{A0s}\ Q_s] = [4\ \frac{kmol}{m^3}\ 0\ \frac{kJ}{hr}]$. In addition, we consider a limitation on the amount of reactant material available over a given operating period $t_p = 1.0\ hr$ (i.e., the amount of reactant material used in each operating period must average to that which would be used under steady-state operation) which is described by the following constraint:

$$\frac{1}{t_p}\int_0^{t_p} u_1(\tau)\ d\tau = 0.0\,kmol/m^3. \tag{11}$$

The stabilizing controller designed for use in scheme 1 of the safety-LEMPC is a Lyapunov-based controller of the form $h(x) = [h_1(x)\ h_2(x)]^T$. The inlet concentration is set to its steady-state value to meet the material constraint of Eq. 11 (i.e., $h_1(x) = 0$). The rate of heat input is determined by the following Sontag control law[32]:

$$h_2(x) = \begin{cases} -\dfrac{L_{\tilde{f}}V + \sqrt{L_{\tilde{f}}V^2 + L_gV^4}}{L_gV}, & \text{if } L_gV \neq 0 \\ 0, & \text{if } L_gV = 0 \end{cases} \tag{12}$$

where $L_{\tilde{f}}V$ and L_gV are the Lie derivatives of the Lyapunov function $V(x)$ with respect to the vector fields $\tilde{f}(x)$ and $g(x)$, respectively. Extensive closed-loop simulations of the CSTR under the Lyapunov-based controller were performed to determine the stability region of the process under $h(x)$ and the corresponding Lyapunov function. A quadratic Lyapunov function of the form $V(x) = x^TPx$ was chosen with P being the following positive definite matrix:

$$P = \begin{bmatrix} 1060 & 22 \\ 22 & 0.52 \end{bmatrix} \tag{13}$$

The stability region was estimated to be the largest level set where the time derivative of the Lyapunov function of the closed-loop system was negative. The stability region of the CSTR under the Lyapunov-based controller, which is used in the Lyapunov-based constraint of Eqs. 7d and 7e, was estimated to be $\rho = 368$ (note that because nominal operation was considered, $\rho_e = \rho$). A sampling period $\Delta = 0.01\ hr$ and an operating period of length $t_f = 1\ hr$ were used to simulate the safety-LEMPC using the interior point solver Ipopt.[33] In addition, for this example, the prediction horizon was chosen to be $N = 10$.

The scheme 1 safety-LEMPC design (Eq. 7 with the additional material constraint of Eq. 11) was applied to the CSTR, with the process states initialized at the stable steady-state, and the process originally operating in Ω_ρ. After half an hour of operation within Ω_ρ, we assume that the safety logic unit determines that it is necessary to reduce the maximum allowable temperature of operation, so it requests a switch of the region of operation from Ω_ρ to $\Omega_{\rho_{sp}}$ where $\rho_{sp} = 294$ (because nominal operation is considered, $\bar{\rho}_{sp} = \rho_{sp}$). Thus, beginning at $t_1 = 0.5\ hr$, the Mode 2 constraint was applied until the closed-loop state was driven into the safety region $\Omega_{\rho_{sp}}$ by decreasing the time derivative of the Lyapunov function by at least as much as the decrease given by the stabilizing control law of Eq. 12. Once the state entered $\Omega_{\rho_{sp}}$, the process was dynamically operated within the safety region to maximize the process profit in this safe region of operation.

The state-space trajectories of the CSTR are presented in Figure 2 and the state and input trajectories are presented in Figure 3. In addition, a plot of the Lyapunov function value of the closed-loop system with respect to time is presented in Figure 4. As can be seen, the scheme 1 safety-LEMPC design maximized the profit before t_1 by driving the state from the steady-state to the boundary of Ω_ρ. At t_1, the level set that defines the Mode 1 and Mode 2 constraints was updated online, and scheme 1 was successfully able to drive the closed-loop state from Ω_ρ to $\Omega_{\rho_{sp}}$ in 19 sampling periods and to optimize the profit within $\Omega_{\rho_{sp}}$, subject to the constraints, thereafter. The drop in the Lyapunov function value at the end of the operating period occurs to satisfy the material constraint (Eq. 11). Although this safety-LEMPC scheme was able to drive the closed-loop state to the safety region $\Omega_{\rho_{sp}}$ in a finite number of sampling periods, the rate of decrease of the Lyapunov function after t_1 was slow, which may not be desirable for safety-critical processes.

Scheme 2: LEMPC with Sufficiently Long Prediction Horizon

As demonstrated by the trajectories of the closed-loop CSTR example under scheme 1, the control actions calculated by scheme 1 are chosen to decrease the Lyapunov function of the closed-loop state but to do so in a manner that optimizes the process economics (rather than optimizing the speed with which the control actions drive the closed-loop state into the safety region), which may cause the time between t_1 and the time at which the state enters $\Omega_{\rho_{sp}}$ to be longer than is practically acceptable. Hence, a scheme that can drive the closed-loop state into $\Omega_{\rho_{sp}}$ by t_1 was developed. This second scheme is an LEMPC design with a sufficiently long prediction

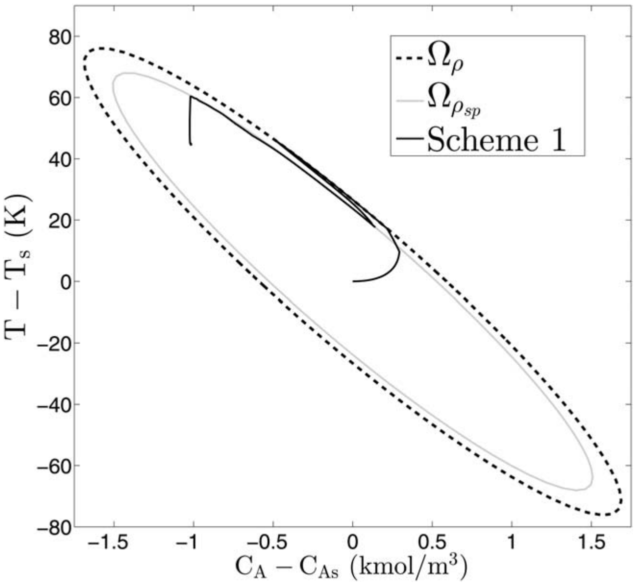

Figure 2. The state-space profile for the closed-loop CSTR under the stabilizing safety-LEMPC design of Eq. 7 (with Eq. 11) for the initial condition $[C_A(0), T(0)]=[1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho=368$.

horizon, a region constraint,[34] and an estimate of the switching time t_1 to drive the closed-loop state into the safety region by t_1 under certain conditions. One of these conditions is that there are no disturbances/uncertainties (i.e., nominal process operation is considered), so the formulation for scheme 2 is presented for the case of nominal operation (i.e., for nominal operation, $\rho_e=\rho$ and no contractive constraint is needed to ensure that the state remains in Ω_ρ since we also assume $x(t_0) \in \Omega_\rho$). The second condition required to prove that scheme 2 can drive the closed-loop state from Ω_ρ into $\Omega_{\rho_{sp}}$ by t_1 is that the switching time is known in advance. The third required condition is that the time interval between the current time and t_1 is long enough in the sense that there exists an explicit stabilizing controller that can drive the closed-loop state into $\Omega_{\rho_{sp}}$ in no more time than this time interval t_1-t_k (the remarks at the end of this section will address the use of scheme 2 when these conditions are not met). Under the assumption that these three conditions are met, the formulation of scheme 2 is as follows:

$$\max_{u \in S(\Delta)} \int_{t_k}^{t_{k+\hat{N}_1+\hat{N}_2}} L_e(\tilde{x}(\tau), u(\tau))\ d\tau \tag{14a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t)=f(\tilde{x}(t), u(t), 0) \tag{14b}$$

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

$$u_i(t) \in U_i,\ \ i=1, \ldots, m,\ \ \forall\ t \in [t_k, t_{k+\hat{N}_1+\hat{N}_2}) \tag{14d}$$

$$\begin{aligned} V(\tilde{x}(t)) \le \hat{\rho},\ \ \forall\ t \in [t_k, t_{k+\hat{N}_1+\hat{N}_2}) \\ \hat{\rho}=\rho,\ \ \forall\ t \in [t_k, t_1) \\ \hat{\rho}=\rho_{sp},\ \ \forall\ t \in [t_1, t_{k+\hat{N}_1+\hat{N}_2}) \end{aligned} \tag{14e}$$

where the prediction horizon N is the summation of two horizons $\hat{N}_1$ and $\hat{N}_2$. $\hat{N}_1$ is initially set to be the number of sampling periods required to drive the closed-loop state into the safety region and it must thus initially be equal to or less than $(t_1-t_0)/\Delta$. $\hat{N}_2$ is an additional number of sampling periods added to the prediction horizon when desired to more closely approximate the infinite-horizon case and thus, for many cases, increase the process profit by choosing control actions that optimize the cost function over a longer period of time.

In the scheme 2 safety-LEMPC formulation presented in Eq. 14, the long prediction horizon, region constraint, and known value of t_1 combine to drive the process state from Ω_ρ into $\Omega_{\rho_{sp}}$ by t_1. Specifically, the region constraint of Eq. 14 allows the nominal process to operate in a time-varying manner within the stability region Ω_ρ at the beginning of process operation. When the process has operated for a sufficient period of time (which depends on the length of the prediction horizon, including whether the initial value of $\hat{N}_1$ is equal to $(t_1-t_0)/\Delta$ or less than it) such that t_1 is within $[t_k, t_{k+\hat{N}_1+\hat{N}_2})$ (i.e., t_1 is within the prediction horizon), the region constraint of Eq. 14e requires that the process state be within $\Omega_{\rho_{sp}}$ by t_1 and that it remains there afterward. Thus, when the optimization problem of Eq. 14 is feasible, the closed-loop state is driven into $\Omega_{\rho_{sp}}$ by t_1. For nominal operation, the closed-loop process state is driven into $\Omega_{\rho_{sp}}$ and maintained there afterward, thus accomplishing Tasks 1 and 2 of the safety-LEMPC design noted in the "Implementation strategy" section. In addition to satisfying safety constraints, all control actions calculated by scheme 2 optimize the process profit subject to the constraints.

The feasibility of the optimization problem in Eq. 14 can be guaranteed when the three conditions previously mentioned, which are the assumptions of nominal operation, the knowledge of t_1 in advance, and that the time interval is longer than the time that it takes a feasible (stabilizing) controller to drive the state into $\Omega_{\rho_{sp}}$, are met. The third requirement can be proven to hold when the initial value of $\hat{N}_1$ is equal to the number of sampling periods required by an explicit stabilizing controller implemented in sample-and-hold that meets the input constraints in Eq. 14d to drive the closed-loop state from any initial state within Ω_ρ to the safety region. However, this number of sampling periods may be large, so that a long prediction horizon may be required, even if the prediction horizon length N is set to its minimum value of $\hat{N}_1$ (i.e., $\hat{N}_2$=0). When the prediction horizon is long, the computation time required to solve the safety-LEMPC dynamic optimization problem may be substantially long and the controller may not be practical to implement.

Remark 6. $\hat{N}_1$ is taken to be the minimum number of sampling periods required to drive the closed-loop state from any initial state in Ω_ρ into $\Omega_{\rho_{sp}}$, although it is only necessary that it is equal to the number of sampling periods required to drive the state from $x(t_1-\hat{N}_1\Delta) \in \Omega_\rho$ to $\Omega_{\rho_{sp}}$ by t_1. However, because $x(t_1-\hat{N}_1\Delta)$ may not be known before the controller is designed and applied, $\hat{N}_1$ should be chosen to be sufficiently large such that $x(t_1-\hat{N}_1\Delta)$ could be any state in Ω_ρ and the process could still be driven to the safety region by t_1.

Remark 7. Because restrictive conditions are required to hold for this scheme to guarantee that the optimization problem is feasible and that the closed-loop state enters $\Omega_{\rho_{sp}}$ by t_1, this scheme may be more difficult to apply practically. However, unlike scheme 1, it has the potential to drive the closed-loop state into $\Omega_{\rho_{sp}}$ by t_1 (rather than starting to move toward $\Omega_{\rho_{sp}}$ after t_1), which may be a desirable property for processes for which changes from one region to another may need to occur by a certain time to ensure process safety.

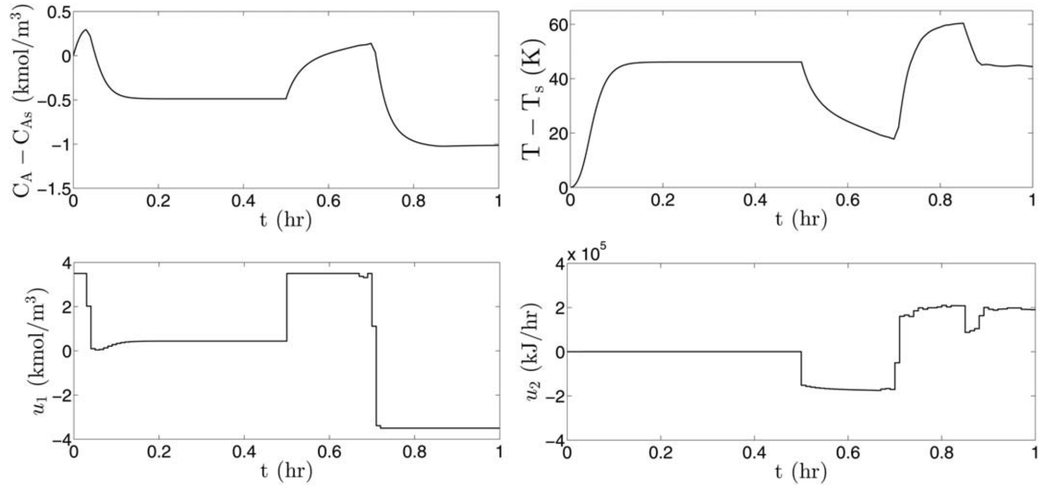

Figure 3. Manipulated input and state profiles for the closed-loop CSTR under the stabilizing safety-LEMPC design of Eq. 7 (with Eq. 11) for the initial condition $[C_A(0), T(0)]=[1.2\ \frac{kmol}{m^3}, 438\ K]$.

Thus, it may be desirable to use scheme 2 even when the restrictive conditions (nominal operation, t_1 is known, and $t_1 - t_k$ is sufficiently long) are not known to hold. When there are disturbances, closed-loop stability and feasibility of scheme 2 cannot be proven, but they may hold. In addition, a contractive constraint like the one used in scheme 1 may be added and applied when no feasible solution is found (although this would not guarantee that the state can still be driven into $\Omega_{\rho_{sp}}$ by t_1). If t_1 is not known and thus it cannot be verified whether $t_1 - t_k$ is sufficiently long, a conservative estimate may be made of t_1, or scheme 2 may be applied long before it is expected that safety concerns may arise.

Remark. 8. The time that an explicit stabilizing controller $h(x)$ may take to drive the closed-loop state into $\Omega_{\rho_{sp}}$ can be known for a specific $h(x)$ (e.g., Sontag's controller). Specifically, the nonlinear process of Eq. 1 can be simulated offline, applying $h(x)$ in a sample-and-hold fashion to measure the length of time that $h(x)$ requires to move any initial state within the stability region (i.e., $x(t_0) \in \Omega_\rho$) to the safety region.

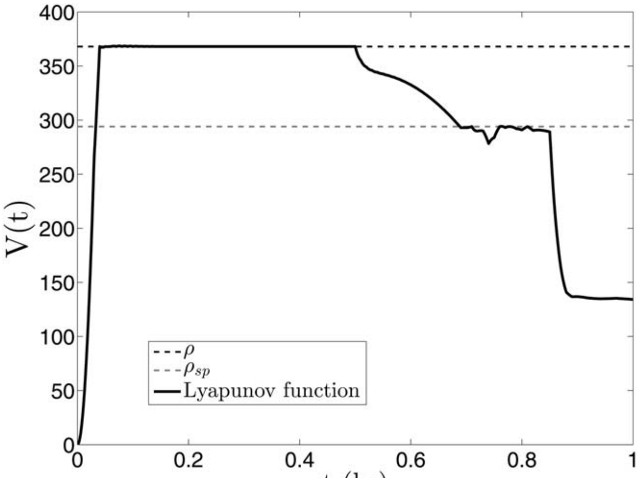

Figure 4. The Lyapunov function value as a function of time for the closed-loop CSTR under the stabilizing safety-LEMPC design of Eq. 7 (with Eq. 11) starting at $[C_A(0), T(0)]=[1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho = 368$ and ending with $\rho_{sp}=294$.

Scheme 2: application to a chemical process example

The same CSTR example that was utilized to demonstrate scheme 1 will now be used to demonstrate scheme 2 (in particular, the same steady-state, initial condition, Lyapunov function $V(x)$, Lyapunov-based controller $h(x)$, input constraints, stability region Ω_ρ, safety level set $\Omega_{\rho_{sp}}$, sampling period, and operating period were used for the process of Eq. 8 with the objective function of Eq. 10 and the material constraint of Eq. 11). For the demonstration of scheme 2 using this example, it is assumed that the safety logic unit indicated at the beginning of the operating period (at t_0) that it is necessary to switch the region of operation to $\Omega_{\rho_{sp}}$ where $\rho_{sp}=294$ after half an hour (i.e., $t_1=0.5\ hr$, which corresponds to 50 sampling periods). As mentioned, this scheme is guaranteed to be feasible as long as the interval $t_1 - t_0$ is long enough in the sense that it is no shorter than the minimum number of sampling periods needed for a stabilizing controller that meets the input constraints and is implemented in sample-and-hold to drive the closed-loop state from the initial state within Ω_ρ to $\Omega_{\rho_{sp}}$ within $t_1 - t_0$. Because the length required for this interval is unknown without performing extensive off-line simulations as noted in Remark 8, the prediction horizon $N=\hat{N}_1+\hat{N}_2$ was set to 100. This ensures that if the number of sampling periods required by an explicit stabilizing controller to drive the closed-loop state into $\Omega_{\rho_{sp}}$ in the interval $t_1 - t_0$ is no more than 50 (because $(t_1 - t_0)/\Delta = 50$), the optimization problem is feasible, and the prediction horizon includes a significant number of additional sampling periods for more economically optimal process performance. The simulations demonstrated that this horizon length was sufficient, because the optimization problem was feasible. Scheme 2 was implemented with a shrinking horizon in this example (the horizon length decreases by 1 at each sampling time t_k until it becomes 0 at t_f).

The closed-loop state-space trajectories of the CSTR temperature and concentration under the scheme 2 safety-LEMPC are presented in Figure 5. In addition, the closed-loop trajectories of the inputs and states under scheme 2 and the corresponding values of the Lyapunov function throughout the

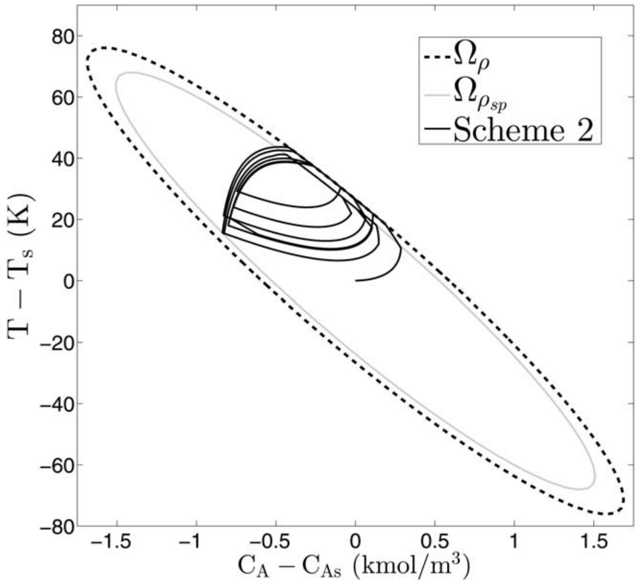

Figure 5. The state-space profile for the closed-loop CSTR under the long-horizon safety-LEMPC design of Eq. 14 (with Eq. 11) for the initial condition $[C_A(0), T(0)]=[1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho=368$.

operating window $t_f=1\ hr$ are shown in Figure 6 and in Figure 7, respectively. The oscillatory behavior of the states and inputs observed in these figures results because scheme 2 seeks to maximize the process profit using a sufficiently long prediction horizon while still meeting process and safety constraints, and the safety-LEMPC determined that the oscillatory trajectories achieved this in the most economically optimal manner. In addition, Figure 5 shows the movement of the trajectories from Ω_ρ into $\Omega_{\rho_{sp}}$, and Figure 7 shows that the closed-loop state moved into $\Omega_{\rho_{sp}}$ by t_1 and was maintained within the safety region thereafter. Thus, scheme 2 was able to achieve economically optimal process operation while driving the closed-loop state into $\Omega_{\rho_{sp}}$ by t_1. However, despite these successes, it required a significant computation time and advance knowledge of t_1, which may not be practical in engineering applications.

Scheme 3: Simultaneous Control of Safety Constraint Sets and Process Economic Optimization

Given the drawbacks of schemes 1 and 2 of the safety-LEMPC (scheme 1 does not guarantee a fast rate of transition of the closed-loop state to the safety region, and scheme 2 requires knowledge of the time that the closed-loop state should be within the safety region in advance and may require a long computation time), a scheme that is able to accomplish the transition of the closed-loop state between the level sets efficiently without requiring prior knowledge of the switching time was developed. This third scheme of the safety-LEMPC incorporates time-varying safety constraints (it adds auxiliary optimization variables that allow the upper bound on the Lyapunov function in the Mode 1 constraint to vary in time) and also adds a penalty in the objective with parameters that can be tuned to achieve a desired rate of transition of the closed-loop state to the safety region without the need for a long prediction horizon to ensure feasibility/stability and without requiring prior knowledge of the switching time. In this section, two formulations of scheme 3 are presented with different time-varying constraints: one that utilizes slack variables to adjust the Lyapunov function bound, and a second that decreases the upper bound on the Lyapunov function dynamically.

Scheme 3-1: slack variable safety level set constraint

In the first formulation of scheme 3, a slack variable is incorporated in the Mode 1 constraint of the LEMPC, and a penalty on the magnitude of the slack variable is imposed in the objective function to drive the closed-loop state to the safety region at a desired rate. The scheme 3 formulation which incorporates this slack variable is presented as follows:

$$\max_{u,s\in S(\Delta)} \int_{t_k}^{t_{k+N}} [L_e(\tilde{x}(\tau),u(\tau)) - a_L s(\tau)^2]\ d\tau \tag{15a}$$

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

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

$$u_i(t)\in U_i,\ \ i=1,\ldots,m,\ \ \forall\ t\in[t_k,t_{k+N}) \tag{15d}$$

$$s(t)\le 0,\ \ \forall\ t\in[t_k,t_{k+N})\ \text{if}\ t_k\ge t_1\ \text{and}\ x(t_k)\notin\Omega_{\rho_{sp}} \tag{15e}$$

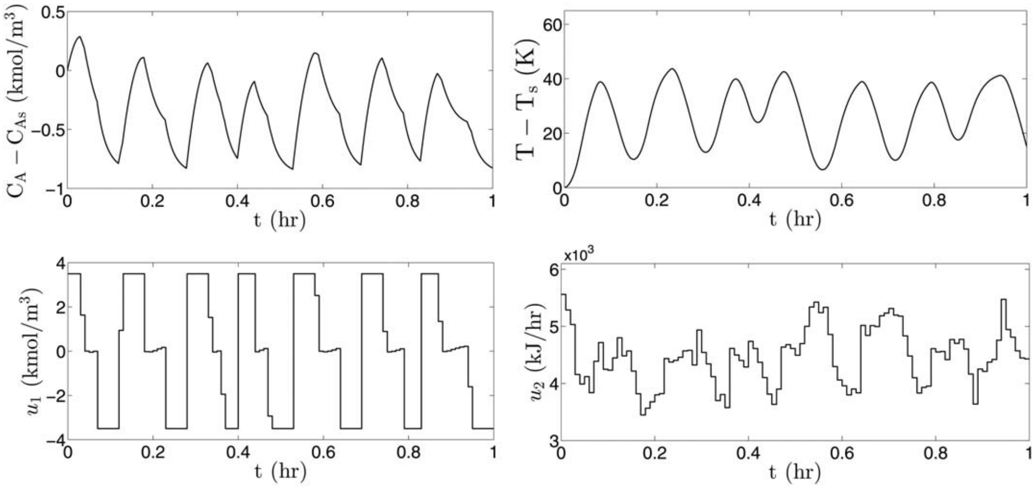

Figure 6. Manipulated input and state profiles for the closed-loop CSTR under the long-horizon safety-LEMPC design of Eq. 14 (with Eq. 11) for the initial condition $[C_A(0), T(0)]=[1.2\ \frac{kmol}{m^3}, 438\ K]$.

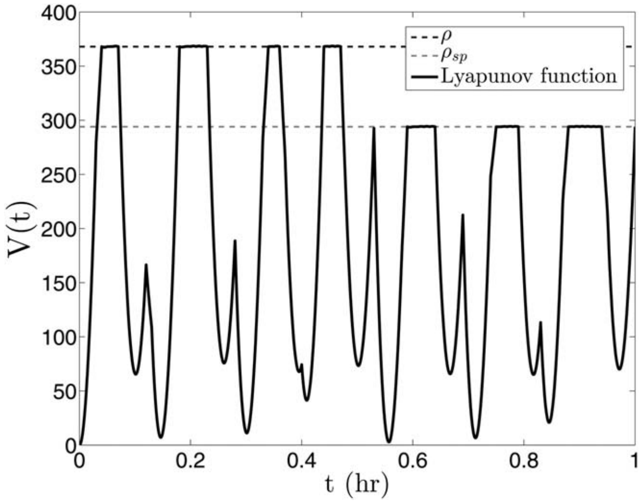

Figure 7. The Lyapunov function value as a function of time for the closed-loop CSTR under the long-horizon safety-LEMPC design of Eq. 14 (with Eq. 11) starting at $[C_A(0), T(0)]=[1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho=368$ and ending with $\rho_{sp}=294$.

$$s(t)=0,\ \forall\ t \in [t_k, t_{k+N})\ \text{if}\ t_k < t_1,\ \text{or if}\ t_k \geq t_1\ \text{and}\ x(t_k) \in \Omega_{\rho_{sp}} \tag{15f}$$

$$\begin{aligned} &V(\tilde{x}(t))+s(t) \leq \hat{\rho},\ \forall\ t \in [t_k, t_{k+N}) \\ &\hat{\rho}=\rho,\ \forall\ t \in [t_k, t_{k+N})\ \text{if}\ t_k < t_1 \\ &\hat{\rho}=\rho_{sp},\ \forall\ t \in [t_k, t_{k+N})\ \text{if}\ t_k \geq t_1 \end{aligned} \tag{15g}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0)$$
$$\text{if}\ x(t_k) \notin \Omega_{\rho_e}\ \text{and}\ t_k < t_1\ \text{or}\ x(t_k) \notin \Omega_{\bar{\rho}_{sp}}\ \text{and}\ t_k \geq t_1 \tag{15h}$$

where s denotes the piecewise constant slack variable of the optimization problem over the prediction horizon $N\Delta$, and a_L is a weighting constant.

From the formulation of scheme 3 in Eq. 15, it can be seen that like scheme 1, scheme 3 optimizes the process economics within Ω_ρ until t_1 (the slack variable is set to $s(t)=0$ in Eq. 15f before t_1, so the safety-LEMPC reduces to the standard formulation of LEMPC in Eq. 6 in that case). At t_1, the safety constraints of Eqs. 15e, 15g, and 15h are activated. Thus, at t_1, the contractive constraint of Eq. 15h begins to be enforced, and it is enforced until the closed-loop state enters $\Omega_{\bar{\rho}_{sp}}$ to ensure that the Lyapunov function always decreases between two sampling periods when the closed-loop state is outside $\Omega_{\bar{\rho}_{sp}}$ (this ensures that Tasks 1 and 2 of the safety-LEMPC strategy from the "Implementation strategy" section are accomplished). In addition, the upper bound $\hat{\rho}$ in Eq. 15g is changed to ρ_{sp} at t_1, and the slack variable is allowed to take negative values. The role of the slack variable in this constraint is to ensure feasibility of the optimization problem. If the slack variable was not included in Eq. 15g, the optimization problem may be infeasible at t_1 because the closed-loop state was allowed to vary throughout all of Ω_ρ before t_1, and thus it would not in general be expected that $x(t_1) \in \Omega_{\rho_{sp}}$. Because of this, the slack variable, which takes a negative value per Eq. 15e, is added to the value of $V(\tilde{x}(t))$, $t \in [t_k, t_{k+N})$ to decrease the left-hand side of Eq. 15g so that the upper bound ρ_{sp} can be met. Thus, this scheme enforces the decrease of the Lyapunov function level set as a soft constraint.

An important role of the slack variable is to ensure feasibility of the optimization problem when the safety logic unit requires the region of operation to change. The second role of the slack variable is to cause the safety-LEMPC to compute control actions that drive the closed-loop state into $\Omega_{\rho_{sp}}$ as quickly as possible when desired. This is a result of its appearance in the objective of Eq. 15a as a term that decreases the value of the objective function and thus it causes the safety-LEMPC to seek control actions that make the magnitude of $s(t)$ as small as possible to maximize the objective function value when the weighting constant a_L is sufficiently large. From Eq. 15g, the magnitude of $s(t)$ will be smaller as $V(\tilde{x}(t))$ becomes closer to ρ_{sp}, and finally takes its minimum magnitude of zero when $V(x(t_k))=\rho_{sp}$. Thus, for a sufficiently large a_L, the use of the slack variable dictates scheme 3-1 to choose control actions that improve the rate of transition to $\Omega_{\rho_{sp}}$ compared to the rate which would be obtained if only the contractive constraint of Eq. 15h were used. The rate of decrease of the level set value is adjusted by varying the weighting constant a_L.

Remark 9. a_L is a weighting constant that determines the rate at which the closed-loop state goes to $\Omega_{\rho_{sp}}$ by penalizing the magnitude of the slack variable in the objective. Due to the penalty in the objective function and the constraint of Eq. 15g, the optimal value of the slack variable at each sampling time when $t_k \geq t_1$ and $x(t_k) \notin \Omega_{\rho_{sp}}$ will be equal to $\rho_{sp} - V(\tilde{x}(t_j))$, where $\tilde{x}(t_j)$ is the predicted state that gives the maximum value of the Lyapunov function in a given sampling period. If it is desired to move quickly toward the safety region regardless of whether or not this decreases the process profit, then a_L must be sufficiently large in the sense that it must dominate the economics-based component $L_e(\tilde{x}, u)$ of the objective function.

Remark 10. The formulation of Eq. 15 implements the slack variable carefully so that issues with closed-loop stability cannot occur due to the slack variable. In this remark, we clarify some of the important aspects of the formulation in Eq. 15. First, the reason that $s(t)=0$ when the state is not transitioning between Ω_ρ and $\Omega_{\rho_{sp}}$ is that if a_L is small, there is a potential that the economic benefit of increasing the magnitude of $s(t)$ to operate the process in a larger region of operation may outweigh the loss in the objective function from the addition of the term containing the slack variable (as an extreme case, a_L may be set to 0 if it is desired to only optimize the process economics, and then the slack variable magnitude may become arbitrarily large to maximize the economics). By setting $s(t)=0$ when the state is within the safety region, such issues cannot occur during operation within the safety region. When the state is transitioning to the safety region, the use of the contractive constraint throughout the transition period ensures that none of the implemented control actions (i.e., the control actions corresponding to the first sampling period in the prediction horizon) will cause the closed-loop state to leave Ω_ρ or to move away from the safety level set, regardless of the values of a_L and of $s(t)$, $t \in [t_k, t_{k+N})$; however, it cannot be guaranteed that control actions for the remaining $N-1$ sampling periods of the prediction horizon (for which the contractive constraint is not imposed) will not cause undesirable behavior for $s(t)$, $t \in [t_{k+1}, t_{k+N})$ if a_L is small. Because these $N-1$ control actions are never implemented, their behavior cannot affect whether the implemented control actions move the state to a lower level set, but it may affect the economic optimality or constraint satisfaction of the process if, for example, constraints that depend on past control actions are included (and if infeasibility occurs, such that even the contractive constraint is not satisfied by the LEMPC solution, it may be necessary to use a different controller such as the Lyapunov-based controller to ensure that the state can be driven to lower level sets, although this may not satisfy process constraints). Therefore, it is necessary to tune a_L carefully or, if there are concerns that it cannot be tuned in such a way to guarantee that the slack variables do not pose an issue for the process, the contractive constraint of Eq. 15h can be enforced at each sampling period of the prediction horizon, which will ensure that all predicted control actions decrease the value of the Lyapunov function and can prevent infeasibility in later sampling periods if the optimization problem is properly formulated. If this issue is accounted for, a_L can be tuned to achieve the desired rate of approach to the safety region. If $a_L = 0$, the slack variable formulation puts more emphasis on the optimization of economics during the approach to the safety region than the speed of approach to the safety region; as a_L is increased, the slack variable formulation will drive the state more quickly to the safety region, within the possible speed of the dynamics of the process and any state/input constraints. An advantage of this slack variable formulation over scheme 1 is that it has greater flexibility because it can be used to maximize profit during the approach to the safety region or used for the alternate purpose of improving the speed of approach to the safety region; a disadvantage, however, is that it requires the addition of additional optimization variables to do so, which may increase the computation time.

Remark 11. In the formulation in Eq. 15, the slack variable is shown as a negative number added to the left-hand side of Eq. 15g to decrease the left-hand side to be below ρ_{sp} after t_1. An alternative way to consider this constraint is to instead require that the slack variables be positive, and to add them to the right-hand side of Eq. 15g, instead of to the left. This increases the bound on the right-hand side so that the value of the Lyapunov function at $\tilde{x}(t)$ is within this upper bound.

Remark 12. In the formulation of Eq. 15, the slack variable $s(t)$ is calculated at every sampling period in the prediction horizon. However, one may consider updating $s(t)$ less often than once per sampling period (e.g., having one slack variable for the entire prediction horizon) to reduce the number of optimization variables, since only the first control action of the prediction horizon is applied. However, a careful analysis should be performed when one slack variable is used over the prediction horizon due to the bound $\rho_{sp}-V(\tilde{x}(t_j))$ on the slack variable that was mentioned in Remark 9. To further clarify, this bound implies that if one slack variable is used for the entire prediction horizon and it is desired to move the closed-loop state to the safety region quickly (i.e., a_L is large), then depending on how this constraint is imposed in the controller, the slack variable $s(t)$ may be ineffective at accomplishing its purpose of causing the implemented control action to move the closed-loop state from Ω_ρ to $\Omega_{\rho_{sp}}$ at a rate faster than that given by the Lyapunov-based controller.

To see this, consider first the extreme case in which the constraint of Eq. 15g is enforced at every time instance in the prediction horizon, including the sampling time t_k at the beginning of the prediction horizon, when the state is transitioning from Ω_ρ to $\Omega_{\rho_{sp}}$. However, $s(t)$ takes only one value for $t \in [t_k, t_{k+N})$ since we are considering the case that one slack variable is used for the whole prediction horizon. In a best case, the value of the Lyapunov function will never become greater than its initial value $V(x(t_k))$ throughout the prediction horizon because it is desired to move all predicted control actions toward the safety level set. Then, because the constraint of Eq. 15g must be satisfied at t_k since it is enforced at that time, and the value of $V(x(t_k))$ is the maximum value of $V(\tilde{x}(t))$ throughout the prediction horizon, the controller will choose $s(t)=\rho_{sp}-V(x(t_k))$, $t \in [t_k, t_{k+N})$ to make the bound of Eq. 15g as tight as possible to minimize the value of $s(t)$ and maximize the objective (since a_L is large). This means that the value of the slack variable is set by the measured state $x(t_k)$, which is not able to be adjusted by the controller, so the penalty term in the objective becomes a constant depending on a measured value of the closed-loop state and thus is ineffective at driving the state into $\Omega_{\rho_{sp}}$ as quickly as possible (the objective in this case is equivalent to using only $L_e(\tilde{x}, u)$, so as for scheme 1, the maximization of economics during the approach to the safety region will slow the approach). Since the Lyapunov function decreases throughout the first sampling period due to the contractive constraint of Eq. 15h and only the first sampling period of the prediction horizon is implemented on the process, it is desirable to make the value of the Lyapunov function at the end of the first sampling period as small as possible to move the closed-loop state as quickly as possible to the safety region, which can be obtained by enforcing the constraint of Eq. 15g at the end of the first sampling period, rather than at any other point during that sampling period.

Scheme 3-1: application to a chemical process example

To demonstrate scheme 3-1, the formulation of Eq. 15 (with the added material constraint) was applied to the same CSTR example that was utilized previously to demonstrate schemes 1 and 2. The optimization variables were the manipulated inputs as well as one slack variable that was held constant throughout the prediction horizon $N = 10$ (one slack variable was used to avoid having a large number of optimization variables that might increase the computation time as in scheme 2). The weighting coefficient was chosen to be $a_L = 80$ to severely penalize the slack variable term in the objective function when the closed-loop state is transitioning between Ω_ρ and $\Omega_{\rho_{sp}}$. Due to this significant weight, the constraint of Eq. 15e was enforced for all times (Eq. 15f was not used).

In this demonstration of scheme 3-1, the process is initially operated in Ω_ρ. After half an hour of operation in Ω_ρ, it is assumed that the safety logic unit determines that it is necessary to switch to the safety region $\Omega_{\rho_{sp}}$ (t_1=0.5 hr). After t_1, the safety-LEMPC calculates control actions that quickly drive the closed-loop state into $\Omega_{\rho_{sp}}$ due to the significant penalty term on the magnitude of the slack variable in the objective function. Figures 8, 9, and 10 depict the state-space trajectories, state and input trajectories, and Lyapunov function value, respectively, for the CSTR operated under scheme 3-1. Figure 8 shows the transition of the closed-loop state from Ω_ρ into $\Omega_{\rho_{sp}}$, and Figure 10 shows that the controller was able to drive

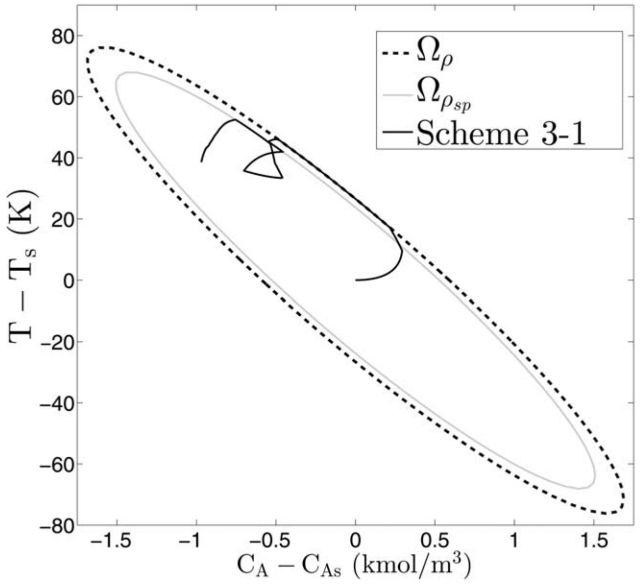

Figure 8. The state-space profile for the closed-loop CSTR under the slack variable safety-LEMPC design of Eq. 15 (with Eq. 11) for the initial condition $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho = 368$.

the closed-loop state into the safety region in 2 sampling periods after t_1 and maintain it within the safety region thereafter. From these figures, it is observed that scheme 3-1 effectively drove the state to the desired safety region rapidly. In addition, this scheme was not computationally expensive and did not require prior knowledge of the switching time.

Remark 13. Based on the discussion in Remark 12, it should be noted that the one slack variable in this example was implemented by enforcing the Mode 1 constraint at the end of each sampling period of the prediction horizon to avoid the issues noted in that remark.

Scheme 3-2: dynamic safety level set

The motivation of the second formulation of scheme 3, termed dynamic safety level set-LEMPC (DSLS-LEMPC), is to design a controller that explicitly controls the rate at which the closed-loop state goes to the safety region $\Omega_{\rho_{sp}}$ while maximizing the process economics. The DSLS-LEMPC design utilizes the explicit stabilizing controller $h(x)$ and dynamic safety-based constraints that decrease the upper bound on the Lyapunov function through an ordinary differential equation to drive the closed-loop state into the safety region at a desired rate while maintaining closed-loop stability and recursive feasibility of the system of Eq. 1 under the DSLS-LEMPC design in the presence of uncertainty. In addition to optimizing the process economic performance, the DSLS-LEMPC paradigm, like the other schemes presented, performs Tasks 1 and 2 of the safety-LEMPC noted in the "Implementation strategy" section.

The optimization problem of the proposed DSLS-LEMPC for the process of Eq. 1 is presented for the case that t_1 has been reached, and is as follows:

$$\max_{u(t),K_c(t)\in S(\Delta)} \int_{t_k}^{t_{k+N}} [L_e(\tilde{x}(\tau),u(\tau)) - \phi(\rho_{sp} - \tilde{\rho}(\tau))]d\tau \tag{16a}$$

$$\text{s.t.}\quad \dot{\tilde{x}}(t) = f(\tilde{x}(t),u(t),0) \tag{16b}$$

$$u_i(t) \in U_i,\ i=1,\ldots,m,\ \forall t \in [t_k,t_{k+N}) \tag{16c}$$

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

$$K_c(t) \geq 0,\ \forall t \in [t_k,t_{k+N}) \tag{16e}$$

$$V(\tilde{x}(t)) \leq \tilde{\rho}(t),\ \forall t \in [t_k,t_{k+N}) \tag{16f}$$

$$\frac{d\tilde{\rho}}{dt} = K_c(t)(\rho_{sp} - \tilde{\rho}(t)) \tag{16g}$$

$$\begin{aligned} &\tilde{\rho}(t_k) = V(x(t_k)), \quad \text{if } x(t_k) \notin \Omega_{\rho_{sp}} \\ &\tilde{\rho}(t_k) = \rho_{sp}, \quad \text{if } x(t_k) \in \Omega_{\rho_{sp}} \end{aligned} \tag{16h}$$

$$\begin{aligned} &\frac{\partial V(x(t_k))}{\partial x} f(x(t_k),u(t_k),0) \\ &\leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k),h(x(t_k)),0), \\ &\text{if } x(t_k) \in \Omega_\rho/\Omega_{\tilde{\rho}_{sp}} \quad \text{or} \quad t_k > t_s \end{aligned} \tag{16i}$$

where t_s is the time after which the DSLS-LEMPC starts to drive the closed-loop state into a small neighborhood of the origin in the presence of disturbances, which will be elaborated on in the "Feasibility and stability analysis" section (in the previous safety-LEMPC schemes, t_s was not included for

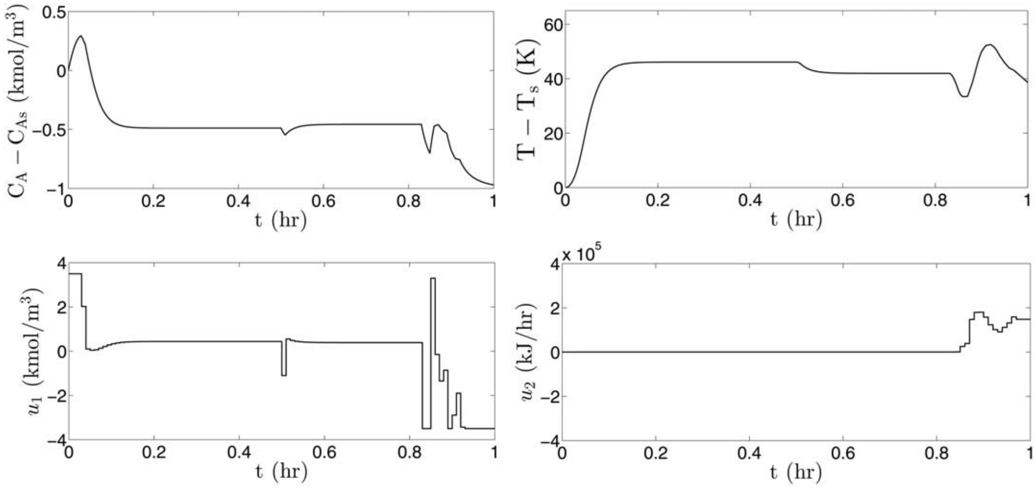

Figure 9. Manipulated input and state profiles for the closed-loop CSTR under the slack variable safety-LEMPC design of Eq. 15 (with Eq. 11) for the initial condition $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$.

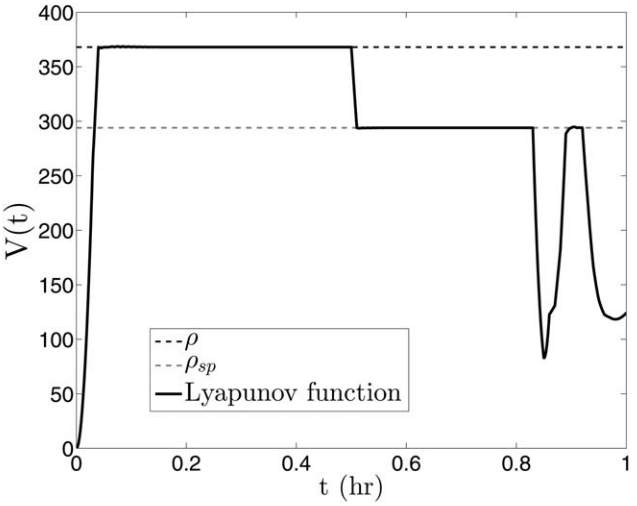

Figure 10. The Lyapunov function value as a function of time for the closed-loop CSTR under the slack variable safety-LEMPC design of Eq. 15 (with Eq. 11) starting at $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho = 368$ and ending with $\rho_{sp} = 294$.

simplicity of presentation and thus was assumed to be infinity; it has been included here to simplify the discussion of the feasibility and closed-loop stability properties of the safety-LEMPC's that will be given in the "Feasibility and stability analysis" section based on this scheme 3-2 formulation). In addition to the manipulated input $u(t)$, the piecewise constant gain $K_c(t)$ is a decision variable of the optimization problem defined over the prediction horizon $N\Delta$. The function $\phi(\cdot)$ is appropriately chosen to give a desired rate of approach of the closed-loop state to $\Omega_{\rho_{sp}}$ (it may be, for example, the squared absolute value of its arguments). The constraint of Eq. 16e restricts the gain $K_c(t)$ to take nonnegative values over the prediction horizon. The DSLS-LEMPC optimization problem minimizes the stage cost $L_e(\tilde{x}(\tau), u(\tau))$, derived from the system economics, and the penalty $\phi(\rho_{sp} - \tilde{\rho}(t))$ that 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.

The dynamic safety-based constraints in Eqs. 16e–16h control the rate of variation of the level set of the predicted Lyapunov function value $V(\tilde{x}(t))$ over the prediction horizon to shrink the region of operation to $\Omega_{\rho_{sp}}$. Specifically, the constraint of Eq. 16f maintains the predicted state trajectory $\tilde{x}(t)$ in the region $\Omega_{\tilde{\rho}(t)}$ over the prediction horizon. The level set $\Omega_{\tilde{\rho}(t)}$ of the predicted Lyapunov function changes with time through the first-order differential equation of Eq. 16g. The gain $K_c(t)$ adjusts the rate of decrease of the level set $\Omega_{\tilde{\rho}(t)}$ over the prediction horizon. The initial condition of Eq. 16g is obtained from the value of the Lyapunov function at the current state if the current state is outside the safety region $\Omega_{\rho_{sp}}$; however, if the current state enters the safety region (i.e., $x(t_k) \in \Omega_{\rho_{sp}}$) then the initial condition will be set to the safety set-point ρ_{sp} (Eq. 16h). The contractive constraint (Eq. 16i) forces the control actions computed by the DSLS-LEMPC to decrease the Lyapunov function for the first sampling period in the prediction horizon by at least as much as the decrease given by the explicit stabilizing controller $h(x)$. Because of the safety-based constraints and the contractive constraint, it is guaranteed that the Lyapunov function value will decrease for the first sampling period (i.e., $V(x(t_{k+1})) \leq V(x(t_k))$). This continuous decreasing of the Lyapunov function value guarantees that the closed-loop state will be driven into the safety region in finite time, which accomplishes Task 1 of the safety-LEMPC. Moreover, to achieve boundedness of the closed-loop state within the safety region $\Omega_{\rho_{sp}}$ and thus, meet the requirement of Task 2, the contractive constraint of Eq. 16i will force the closed-loop state into the subset of the safety region $\Omega_{\hat{\rho}_{sp}} \subset \Omega_{\rho_{sp}}$ which makes the region $\Omega_{\rho_{sp}}$ a forward invariant set.

Remark 14. The contractive constraint of Eq. 16i is imposed in the optimization problem to ensure that $\tilde{\rho}(t)$ is decreasing at the beginning of each sampling period t_k in the presence of disturbances, and the role of the constraints in Eqs. 16e–16h in this case is to enhance the rate of decrease of $\tilde{\rho}(t)$ over the prediction horizon. However, the constraints of Eqs. 16e–16h will decrease $\tilde{\rho}(t)$ without the need to impose the contractive constraint (Eq. 16i) for the nominal system of Eq. 1 (i.e., $w(t) \equiv 0$) under the DSLS-LEMPC design when the gain $K_c(t)$ is sufficiently large over the prediction horizon.

Remark 15. Owing to the constraint of Eq. 16h, the penalty term $\phi(\rho_{sp} - \tilde{\rho}(t))$ in the objective function of the optimization problem of Eq. 16 will be equal to zero and the upper bound of the predicted Lyapunov function value in Eq. 16f will be set to the safety set-point ρ_{sp} once $x(t_k)$ enters the safety region $\Omega_{\rho_{sp}}$. From that point on, due to the contractive constraint of Eq. 16i, $\Omega_{\rho_{sp}}$ will be a forward invariant set (which will be proven in the "Feasibility and stability analysis" section).

Remark 16. If the penalty term $\phi(\rho_{sp} - \tilde{\rho}(t))$ is large relative to the process economic cost, it will be desirable that $\tilde{\rho}(t) = \rho_{sp}$, which means that it is preferable to go as quickly as possible to $\Omega_{\rho_{sp}}$ and then optimize the profit after the closed-loop state enters the safety region, rather than optimizing it along the way. Thus, the weighting on the economics-based part of the objective function compared to that of the safety-based penalty may depend on the process and how long in advance of a fault or change in the process conditions the controller is notified that it needs to change the region of operation to $\Omega_{\rho_{sp}}$.

Remark 17. Note that the decrease of $\tilde{\rho}(t)$ through Eq. 16g does not mean that the value of the Lyapunov function of the actual state $V(x(t))$ has decreased according to Eq. 16g. This is due to process disturbances and also the fact that $V(x)$ is a separate function for which the dynamics are not those in Eq. 16g. However, if $K_c(t)$ and $u(t)$ can be found that can decrease $\tilde{\rho}(t)$ in Eq. 16f, the predicted state is guaranteed to be within smaller level sets. If $\tilde{\rho}(t)$ decreases quickly, this means that there is a value of $u(t)$ that can quickly decrease $V(\tilde{x}(t))$ and thus is likely to decrease $V(x(t))$ significantly, even if it is not able to decrease it by as much as is indicated by Eq. 16f due to disturbances in the actual process.

Remark 18. Unlike the piecewise constant input $u(t)$ which is, for practical implementation reasons, implemented in a sample-and-hold fashion, $K_c(t)$ can be updated as often as desired because it is an auxiliary variable for optimization purposes and not a control action that is implemented by the actuator, and thus there is no limit on how often it can be updated; however, constant updating (e.g., every integration step) in general is not computationally practical.

Remark 19. It was noted that the DSLS-LEMPC formulation was presented for the case that t_1 had already been reached, and it is desired to move the state into $\Omega_{\rho_{sp}}$, to provide better clarity to the discussion of the scheme by explicitly including ρ_{sp} in the formulation of Eq. 16. In the time before t_1, the value of ρ_{sp} in Eq. 16 would be replaced by ρ, and the value of $\bar{\rho}_{sp}$ would be replaced by ρ_e, which would simplify Eq. 16 to the standard LEMPC design of Eq. 6. At t_1, the EMPC of Eq. 16 would then be used as written, which would require only an update of the values of ρ_{sp} and $\bar{\rho}_{sp}$ from the safety logic unit.

Remark 20. Scheme 3-1 and scheme 3-2 have many similarities and can be used to accomplish similar goals, although they are not equivalent. They both have the benefit of flexibility compared to schemes 1 and 2 because of the tuning parameters that they incorporate, as noted for scheme 3-1 in Remark 10. Like scheme 3-1, a disadvantage of scheme 3-2 compared to schemes 1 and 2 is that it requires the addition of auxiliary decision variables that may increase the computation time.

There are several differences in the manner in which schemes 3-1 and 3-2 handle the dynamic variation of the upper bound on the Lyapunov function throughout time. For example, the auxiliary optimization variable $K_c(t)$ used in scheme 3-2 is not included in any equation that includes the values of the closed-loop states themselves, but is only used to modify the bound on the Lyapunov function. In addition, it is not utilized in the objective function, so there are no possible negative interactions between $K_c(t)$ and the values of the closed-loop states that would require $K_c(t)$ to be set to a specific value once the state enters the safety region. This is in contrast to scheme 3-1, where the slack variable $s(t)$ is used in the Mode 1 constraint that is also a function of the states and thus can directly affect their values, in addition to being in the objective. This can cause the competing effects noted in Remark 10 that require $s(t)$ to be set to 0 after the state enters the safety region. Another significant difference between the two schemes is that scheme 3-2 controls the upper bound on the Lyapunov function value through the first-order ordinary differential equation that adjusts the bound on the Lyapunov function value $\tilde{\rho}(t)$ in time. Although this differential equation requires a value of the decision variable $K_c(t)$ to modify the Lyapunov function bound, the bound on the Lyapunov function value is not directly calculated by the safety-LEMPC. Thus, scheme 3-2 can be described as adjusting the bound on the level set by using a controller (Eq. 16g) within the safety-LEMPC controller. In contrast, scheme 3-1 modifies the upper bound on the Lyapunov function by adjusting $s(t)$, which is an optimization variable of the safety-LEMPC.

Another difference between the two formulations is that if it is desired to reduce the computation time by applying only one value of the auxiliary variable ($s(t)$ in scheme 3-1 and $K_c(t)$ in scheme 3-2) throughout the prediction horizon, the manner in which $s(t)$ is implemented in such a case is an important consideration in scheme 3-1, as noted in Remark 12, due to the structure of that optimization problem, but no special considerations need to be made for scheme 3-2. Conversely, there may be some benefit with respect to the rate of approach of the closed-loop state to the safety region when the number of optimization variables $K_c(t)$ in scheme 3-2 is increased (i.e., there are more decision variables $K_c(t)$ than the number of sampling periods in the prediction horizon) due to the increase in flexibility that this may give to adjust the upper bound on the Lyapunov function $\tilde{\rho}(t)$ (and thus the greater possibility of finding control actions that move the state to the safety region more quickly). For scheme 3-1, in contrast, there is no benefit to increasing the number of slack variables $s(t)$ because the slack variables set the upper bound on the Lyapunov function directly and when the input is piecewise constant as in the safety-LEMPC schemes, changing the upper bound on the Lyapunov function often throughout a sampling period will not affect the values of the control actions chosen since they are fixed throughout the sampling period.

Remark 21. Unlike scheme 2, schemes 3-1 and 3-2 do not guarantee that the closed-loop state will be within $\Omega_{\rho_{sp}}$ by any specific time. They can be tuned to drive the state into $\Omega_{\rho_{sp}}$ quickly in the sense that they may take the minimum or close to the minimum number of sampling periods possible to drive the closed-loop state into $\Omega_{\rho_{sp}}$ from $x(t_1)$; however, the actual speed of this transition will depend on the process dynamics and state/input constraints, and thus may not, in practice, occur on a short timescale. Scheme 2 had the benefit then that regardless of the speed of the process dynamics and constraints, it can drive the state into $\Omega_{\rho_{sp}}$ by a required time; however, it is not in general possible to prove that it can do this in the presence of disturbances or if t_1 is not known, whereas schemes 3-1 and 3-2 are robust to disturbances and require no prior knowledge of the switching time.

Remark 22. There are no restrictions on the objective functions that can be used with the safety-LEMPC schemes. This means that they hold not only for an economics-based objective, but can also hold for traditional quadratic objectives utilized in tracking MPC in industry.

Feasibility and stability analysis

In this section, we present sufficient conditions such that the state of the closed-loop system of Eq. 1 under the three safety-LEMPC schemes is always bounded in $\Omega_{\rho_{sp}}$ and is ultimately bounded in a compact set containing the origin. We present these results in detail for the DSLS-LEMPC design, and then describe how they can be generalized to the other safety-LEMPC schemes through several remarks. Since the DSLS-LEMPC design is a modified formulation of the classical LEMPC design of,[20] the proofs of stability and feasibility utilize the approach in Ref. 20. We begin the proof for the DSLS-LEMPC by re-stating the two propositions required for stability and feasibility from Ref. 20 to define functions and parameters needed for the proof of feasibility and closed-loop stability of the DSLS-LEMPC formulation.

Proposition 1. (c.f. Refs. 20, 35). *Consider the systems*

$$\begin{aligned} \dot{x}_a(t) &= f(x_a(t), u_1(t), \ldots, u_m(t), w(t)) \\ \dot{x}_b(t) &= f(x_b(t), u_1(t), \ldots, u_m(t), 0) \end{aligned} \tag{17}$$

with initial states $x_a(t_0) = x_b(t_0) \in \Omega_\rho$. There exists a $\mathcal{K}$ function $f_W(\cdot)$ such that

$$|x_a(t) - x_b(t)| \le f_W(t - t_0), \tag{18}$$

for all $x_a(t), x_b(t) \in \Omega_\rho$ and all $w(t) \in W$ with

$$f_W(\tau) = \frac{L_w \theta}{L_x}(e^{L_x \tau} - 1). \tag{19}$$

Proposition 2. (c.f. Refs. 20, 35). *Consider the Lyapunov function $V(\cdot)$ of the system of Eq. 1. There exists a quadratic function $f_V(\cdot)$ such that*

$$V(x) \le V(\hat{x}) + f_V(|x - \hat{x}|) \tag{20}$$

for all $x, \hat{x} \in \Omega_\rho$ with

$$f_V(s)=\alpha_4(\alpha_1^{-1}(\rho))s+M_v s^2 \tag{21}$$

where M_v is a positive constant.

In the following theorem, we establish feasibility and stability of DSLS-LEMPC by introducing conditions on ρ_{sp} and $\bar{\rho}_{sp}$.

Theorem 1. *Consider the system of Eq. 1 in closed-loop under the DSLS-LEMPC design of Eq. 16 based on a controller h(x) that satisfies the conditions of Eq. 2. Let $\epsilon_w > 0$, $\Delta > 0$, $\rho > \rho_{sp} > \bar{\rho}_{sp} > \rho_s > 0$ satisfy*

$$\bar{\rho}_{sp} \le \rho_{sp} - f_V(f_W(\Delta)) \tag{22}$$

and

$$-\alpha_3(\alpha_2^{-1}(\rho_s))+L'_xM\Delta+L'_w\theta \le -\epsilon_w/\Delta. \tag{23}$$

If $x(t_0) \in \Omega_\rho$, $\rho_{\min} \le \bar{\rho}_{sp}$ and $N \ge 1$ where

$$\rho_{\min}=\max\{V(x(t+\Delta)) : V(x(t)) \le \rho_s\}, \tag{24}$$

then the state x(t) of the closed-loop system can be driven in a finite time to $\Omega_{\rho_{sp}}$ and then be bounded there, and also the state x(t) of the closed-loop system is ultimately bounded in $\Omega_{\rho_{\min}}$.

Proof. The proof will be given in two parts. In Part 1, we prove the feasibility of the optimization problem of Eq. 16 for all initial states starting within the region Ω_ρ. In Part 2, we prove the two results of Theorem 1 (which are that the state $x(t)$ of the closed-loop system can be driven in a finite time to $\Omega_{\rho_{sp}}$ and then be bounded there, and also is ultimately bounded in $\Omega_{\rho_{\min}}$). ■

Part 1: The solution $K_c(t)=0, \forall t \in [t_k, t_{k+N})$, $u(t)=h(\tilde{x}(t_n))$, $\forall t \in [t_n, t_{n+1})$ with $n=k,\ldots,N+k-1$ is a feasible solution when $\tilde{x}(t)$ is maintained within Ω_ρ. The gain $K_c(t)=0, \forall t \in [t_k, t_{k+N})$ is feasible since it satisfies Eq. 16e over the prediction horizon. When $K_c(t)=0$, then by Eq. 16g, $\tilde{\rho}(t)$ will be equal to its initial value from Eq. 16h throughout the prediction horizon, and thus the upper bound on the Lyapunov function in Eq. 16f will be fixed (i.e., either $\tilde{\rho}(t_k)=V(x(t_k)) \Rightarrow V(\tilde{x}(t)) \le V(x(t_k))$, $\forall t \in [t_k, t_{k+N})$, if $x(t_k) \notin \Omega_{\rho_{sp}}$ or $\tilde{\rho}(t_k)=\rho_{sp} \Rightarrow V(\tilde{x}(t)) \le \rho_{sp}$, $\forall t \in [t_k, t_{k+N})$, if $x(t_k) \in \Omega_{\rho_{sp}}$). In such a case, 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. 16c and also, because of the closed-loop stability property of the Lyapunov-based controller $h(x)$,[30] it satisfies the constraint of Eq. 16f. Trivially, $u(t)=h(\tilde{x}(t_n)), \forall t \in [t_n, t_{n+1})$ with $n=k,\ldots,N+k-1$ satisfies the contractive constraint of Eq. 16i, making it a feasible input trajectory for the DSLS-LEMPC design of Eq. 16. Therefore, $K_c(t)=0, \forall t \in [t_k, t_{k+N})$, $u(t)=h(\tilde{x}(t_n)), \forall t \in [t_n, t_{n+1})$ with $n=k,\ldots,N+k-1$ is a feasible solution, and recursive feasibility of the DSLS-LEMPC follows if the closed-loop state trajectory is maintained within Ω_ρ (which will be proven in Part 2).

Part 2: We now show that if the closed-loop state $x(t_k)$ is initialized outside the safety region (i.e., $x(t_k) \notin \Omega_{\rho_{sp}}$ and $t_k \le t_s$), then within finite time the closed-loop state will be maintained in $\Omega_{\rho_{sp}}$. We also show that if $t_k > t_s$, then the closed-loop state will be ultimately bounded in a small region containing the origin.

If $x(t_k) \in \Omega_\rho/\Omega_{\bar{\rho}_{sp}}$, then due to the contractive constraint of Eq. 16i in the DSLS-LEMPC formulation of Eq. 16, the Lyapunov function of the closed-loop state will decrease for the first sampling period in the prediction horizon by at least the rate given by the explicit stabilizing controller $h(x)$. Owing to the closed-loop stability property of the explicit controller $h(x)$,[30] the Lyapunov function value of the closed-loop state under the DSLS-LEMPC design will decrease in the next sampling period (i.e., $V(x(t)) \le V(x(t_k)), \forall t \in [t_k, t_{k+1}]$, which is derived in Ref. 20). Thus, if $x(t_k) \in \Omega_\rho/\Omega_{\bar{\rho}_{sp}}$ then $V(x(t_{k+1})) < V(x(t_k))$ and in finite time, the closed-loop state converges to $\Omega_{\bar{\rho}_{sp}}$ (i.e., $x(t_{k+j}) \in \Omega_{\bar{\rho}_{sp}}$ where j is a finite positive integer).

If $x(t_k) \in \Omega_{\bar{\rho}_{sp}}$ and $t_k \le t_s$, then $\tilde{x}(t_{k+1}) \in \Omega_{\bar{\rho}_{sp}}$ by the constraints of Eqs. 16f–16h and $x(t_{k+1}) \in \Omega_{\rho_{sp}}$, which is proven in Ref. 20. If $x(t_k) \in \Omega_{\rho_{sp}}/\Omega_{\bar{\rho}_{sp}}$, then the contractive constraint will continue to be enforced, decreasing the Lyapunov function value until $x(t_{k+l}) \in \Omega_{\bar{\rho}_{sp}}$ where l is a finite positive integer. Therefore, $\Omega_{\rho_{sp}}$ is a forward invariant set.

If $t_k > t_s$, then the contractive constraint of Eq. 16i will continue to decrease the Lyapunov function value until the closed-loop state enters the compact set $\Omega_{\rho_{\min}}$ in which it is ultimately bounded. The proof of this is analogous to the proof of ultimate boundedness in Ref. 20.

Remark 23. As noted in Remark 19, before t_1, the safety-LEMPC operates with ρ_{sp} and $\bar{\rho}_{sp}$ replacing ρ and ρ_e in the formulation of Eq. 16, so scheme 3-2 is also stable before t_1 and ensures closed-loop stability for the same reasons as mentioned in the proof of Theorem 1.

Remark 24. The proofs of feasibility and closed-loop stability of schemes 1, 2, and 3-1, under the assumptions of Theorem 1 that $\Omega_{\rho_{\min}} \subseteq \Omega_{\bar{\rho}_{sp}}$ and that $x(t_0) \in \Omega_\rho$, have many similarities to the proof presented for the DSLS-LEMPC and will be outlined in several following remarks. These remarks will show that schemes 1 and 3-1, like scheme 3-2, have robustness properties that guarantee that they can maintain closed-loop stability of the process state within a given safety region in the presence of sufficiently small disturbances (i.e., disturbances small enough that the Lyapunov-based controller implemented in sample-and-hold is robust to these disturbances) after the state has entered this safety region, and will show that scheme 2 can guarantee that the closed-loop state can be maintained within a given safety region for nominal operation.

Remark 25. For scheme 1, $u(t)=h(\tilde{x}(t_n)), \forall t \in [t_n, t_{n+1})$ with $n=k,\ldots,N+k-1$, is a feasible solution when $t_k < t_1$ and when $t_k \ge t_1$ because it satisfies the input constraints and the Mode 1 and Mode 2 constraints in Eqs. 7c–7e. This scheme is also guaranteed to maintain closed-loop stability of the state before and after t_1. Before t_1, $\hat{\rho}=\rho_e$, and the safety-LEMPC operates as the standard LEMPC in Eq. 6, which is guaranteed to maintain closed-loop stability according to the proof presented in Ref. 20. From t_1 until the state first enters $\Omega_{\bar{\rho}_{sp}}$, the Mode 2 constraint of Eq. 7e is able to drive the closed-loop state from any state in Ω_ρ into $\Omega_{\bar{\rho}_{sp}}$ because of the robustness property of the explicit stabilizing controller, as mentioned in the proof of Theorem 1 for the DSLS-LEMPC. Finally, after the state has reached $\Omega_{\bar{\rho}_{sp}}$, it is maintained within this final level set by the combination of the Mode 1 and Mode 2 constraints in the same manner as was detailed for the DSLS-LEMPC in the proof of Theorem 1.

Remark 26. Feasibility and closed-loop stability for scheme 2 can be proven when the three conditions mentioned in the section "Scheme 2: LEMPC with sufficiently long prediction horizon" are met (nominal process operation, t_1 is known, and the time interval t_1-t_k is longer than $t_1-\hat{N}_1\Delta$, where $\hat{N}_1$ is defined based on an explicit stabilizing controller $h(x)$). When these conditions are met, $u(t)=h(\tilde{x}(t_n)), \forall t \in [t_n, t_{n+1})$ with $n=k,\ldots,N+k-1$ is a feasible solution because it is guaranteed to drive the closed-loop state from $x(t_0) \in \Omega_\rho$ to

$\Omega_{\rho_{\min}}$ in finite time if implemented repeatedly due to the stability properties of the Lyapunov-based controller.[30] Thus, before t_1 is within the prediction horizon, $\hat{\rho}=\rho$ in Eq. 14e and $u(t)=h(\tilde{x}(t_n)), \forall t \in [t_n, t_{n+1})$ with $n=k, \ldots, N+k-1$ is a feasible solution because it decreases the value of $V(x(t))$ with time which ensures that $V(\tilde{x}(t))$ is maintained within Ω_ρ. When t_1 is within the prediction horizon (and thus $\hat{\rho}=\rho$ before t_1 and ρ_{sp} starting at t_1 in Eq. 14e), $u(t)=h(\tilde{x}(t_n)), \forall t \in [t_n, t_{n+1})$ with $n=k, \ldots, N+k-1$ is feasible because the prediction horizon was designed with respect to $h(x)$ to be at least as long as the time needed for an explicit stabilizing controller $h(x)$ implemented in sample-and-hold to drive the closed-loop state into $\Omega_{\rho_{sp}}$ from any point within Ω_ρ while meeting the input constraints of Eq. 14d. Closed-loop stability in the sense of boundedness of the closed-loop state within Ω_ρ before it enters $\Omega_{\rho_{sp}}$ and within $\Omega_{\rho_{sp}}$ after it first enters the safety region is guaranteed for a nominal process operated under scheme 2 when a feasible solution exists because then the constraints of Eq. 14e hold not only in the optimization problem but also for the actual process.

Remark 27. For scheme 3-1, $u(t)=h(\tilde{x}(t_n)), \forall t \in [t_n, t_{n+1})$, $n=k, \ldots, N+k-1$, with $s(t)=0 \ \forall \ t \in [t_k, t_{k+N})$ is a feasible solution before t_1 because it trivially satisfies the contractive constraint and Eq. 15f and also satisfies the constraint of Eq. 15g because $\hat{\rho}=\rho$. When $t_k \geq t_1$ and $x(t_k) \notin \Omega_{\rho_{sp}}$, $u(t)=h(\tilde{x}(t_n)), \forall t \in [t_n, t_{n+1})$, $n=k, \ldots, N+k-1$, with a negative $s(t)$ of arbitrarily large magnitude allows for Eqs. 15e and 15g to be satisfied and also satisfies the contractive constraint and the input constraints by design of $h(x)$. When $t_k \geq t_1$ and $x(t_k) \in \Omega_{\rho_{sp}}$, $\hat{\rho}=\rho_{sp}$, and $u(t)=h(\tilde{x}(t_n)), \forall t \in [t_n, t_{n+1})$, $n=k, \ldots, N+k-1$, with $s(t)=0 \ \forall \ t \in [t_k, t_{k+N})$ is a feasible solution because it again satisfies both the contractive constraint and the constraints of Eqs. 15g and 15f. The proof of the closed-loop stability of this method follows that of the standard LEMPC of Eq. 6 presented in Ref. 20 before t_1. Scheme 3-1 decreases the state to $\Omega_{\bar{\rho}_{sp}}$ in finite time due to the contractive constraint and then maintains the state within $\Omega_{\rho_{sp}}$ after it enters this set for the reasons described for the DSLS-LEMPC in the proof of Theorem 1.

Remark 28. To prove ultimate boundedness of the closed-loop state under schemes 1 and 3-1, the contractive constraint in each scheme could be enforced for all times after a pre-specified time t_s. To prove ultimate boundedness of the closed-loop state under scheme 2, this contractive constraint could be added to scheme 2 at t_s and enforced for all times after t_s. In all three cases, the proof of ultimate boundedness would follow that presented for the DSLS-LEMPC in Part 2 of the proof of Theorem 1.

Scheme 3-2: application to a chemical process example

The DSLS-LEMPC design is demonstrated using the same CSTR example that was used for scheme 1, scheme 2, and scheme 3-1, but with different problem settings. Specifically, the process of Eq. 8 was operated with the same objective function in Eq. 10, the same constraints on the inputs, for $t_f=1 \ hr$, using a prediction horizon $N=10$ and a sampling period $\Delta=0.01 \ hr$. However, the material constraint of Eq. 11 was not used. The process of Eq. 8 was operated around the unstable steady-state point $[C_{As2} \ T_{s2}]=[2 \ \frac{kmol}{m^3} \ 400 \ K]$. Moreover, a quadratic Lyapunov function $V(x)=x^T P x$ was constructed with $P=\text{diag}([636.94 \ 0.5])$ to determine the stability region Ω_ρ for the DSLS-LEMPC design. The weights of the P matrix were chosen so that each state contributed to the Lyapunov function value approximately equally. The stability region was chosen to be the largest level set where the time-derivative of the Lyapunov function, $\dot{V}$, along the closed-loop state trajectories is negative under the Lyapunov-based controller $h(x)=[h_1(x) \, h_2(x)]^T$ defined by feedback linearization as follows:

$$h_1(x)=\frac{V}{F}[-\gamma x_1+\frac{-F}{V}(C_{A0s}-(x_1+C_{As2}))+ \\ k_0 e^{\frac{-E}{R(x_2+T_{s2})}}(x_1+C_{As2})^2]$$

$$h_2(x)=\rho_L C_p V[-\gamma x_2+\frac{-F}{V}(T_0-(x_2+T_{s2}))+ \\ \frac{\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{R(x_2+T_{s2})}}(C_{As2}+x_1)^2]$$

where $\gamma=25$ was chosen to make the process model of Eq. 8 globally exponentially stable under $h(x)$ in the absence of input constraints. Both control laws are subject to the input constraints and by using this strategy, ρ was chosen to be 2002.3.

The change in the example specifications in this section is made to show that the safety-LEMPC schemes have the potential not only to ensure safe operation around a stable steady-state, but also around an unstable steady-state. The examples presented in this work are not intended to be used to directly compare the performance of the schemes for the particular system used, but rather to demonstrate the properties of the individual schemes, since the objective of this work is to develop several safety-LEMPC schemes and to present their differences and similarities so that a control engineer can have an understanding of which scheme may be best for a particular application due to its properties as a formulation.

We assume that at the beginning of operation the safety logic unit determines that it is necessary to shift the region of operation Ω_ρ to the safety region $\Omega_{\rho_{sp}}$ where $\rho_{sp}=500$ (i.e., $t_1=t_0$), again to reduce the maximum allowable temperature of operation. The process of Eq. 8 is controlled by the DSLS-LEMPC design given by the following optimization problem:

$$\min_{u \in S(\Delta), K_c} \int_{t_k}^{t_{k+N}} \left[\frac{-L_e(\tilde{x}(\tau), u(\tau))}{N\Delta}+\frac{|\rho_{sp}-\tilde{\rho}(\tau)|^2}{h_c}\right] d\tau \tag{26a}$$

$$\text{s.t.} \qquad \dot{\tilde{x}}(t)=f(\tilde{x}(t), u(t), 0) \tag{26b}$$

$$u_i(t) \in U_i, \ \ i=1, \ldots, m, \ \ \forall t \in [t_k, t_{k+N}) \tag{26c}$$

$$\tilde{x}(t_k)=x(t_k) \tag{26d}$$

$$K_c \geq 0, \forall t \in [t_k, t_{k+N}) \tag{26e}$$

$$V(\tilde{x}(t)) \leq \tilde{\rho}(t), \forall t \in [t_k, t_{k+N}), \tag{26f}$$

$$\frac{d\tilde{\rho}}{dt}=K_c(\rho_{sp}-\tilde{\rho}(t)) \tag{26g}$$

$$\begin{aligned} \tilde{\rho}(t_k)&=V(x(t_k)), \quad \text{if } x(t_k) \notin \Omega_{\rho_{sp}} \\ \tilde{\rho}(t_k)&=\rho_{sp}, \quad \text{if } x(t_k) \in \Omega_{\rho_{sp}} \end{aligned} \tag{26h}$$

where the optimization variables are the piecewise-constant trajectory for $u(t)$ and the auxiliary optimization variable K_c (only one value of K_c is found for the entire prediction horizon to minimize the number of auxiliary optimization variables used), and h_c is the integration time step $10^{-5} \ hr$.

The DSLS-LEMPC formulation considered is implemented with a prediction horizon $N=10$. The objective function of the optimization problem includes two terms; the first term is

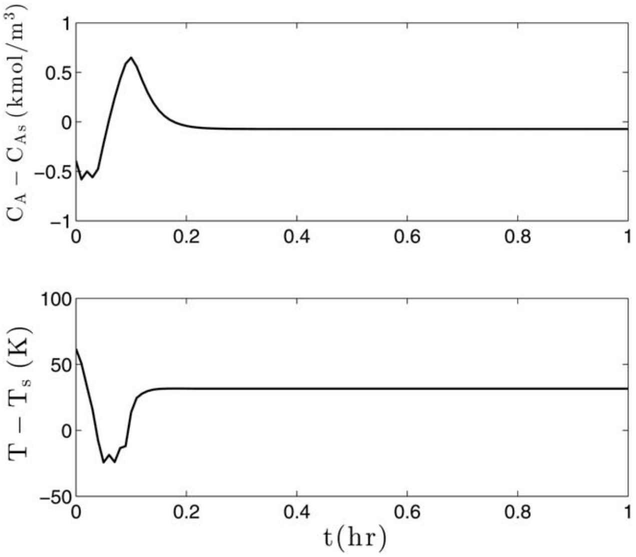

Figure 11. The state profiles for the closed-loop CSTR under the DSLS-LEMPC design of Eq. 26 for the initial condition $[C_A(0), T(0)]=[1.606\ \frac{kmol}{m^3}, 461.7\ K]$.

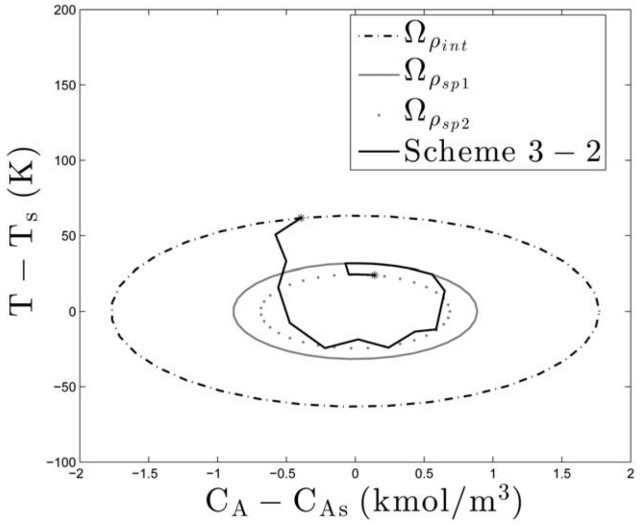

Figure 13. The state-space profile for the closed-loop CSTR under the DSLS-LEMPC design of Eq. 26 for the initial condition $[C_A(0), T(0)]=[1.606\ \frac{kmol}{m^3}, 461.7\ K]$ and $\rho_{int}=2002.3$ for two different safety set-points $\rho_{sp1}=500$ at $t_1=0$ hr, $\rho_{sp2}=300$ at $t_2=0.5$ hr.

the negative of the time-average production rate of Eq. 10 (to maximize the production rate since Eq. 26 is a minimization problem), and the second term is the L^2 norm of the difference between $\tilde{\rho}(t)$ and the safety set-point ρ_{sp}. We penalize the second term significantly more than the average production rate using a large weight $1/h_c$ so that the highest priority of the DSLS-LEMPC is to drive the closed-loop state into the safety region $\Omega_{\rho_{sp}}$ in a short time.

In the following simulation, we demonstrate the application of the proposed DSLS-LEMPC by starting the optimization problem from an initial condition that is at the boundary of the stability region Ω_ρ (significantly far from the safety region) to assess the quality of the DSLS-LEMPC controller. Figures 11 and 12 show the closed-loop state trajectories and the manipulated input trajectories of the dynamic model of Eq. 8 under the DSLS-LEMPC design of Eq. 26. Due to the high penalty in the objective function on the deviation of the predicted states from the safety region $\Omega_{\rho_{sp}}$, the manipulated heat rate u_2 drops to its minimum allowable value at the beginning of the operating period to decrease the temperature of the reactor x_2 as quickly as possible so that the closed-loop trajectories enter the safety region in a short time. Once the closed-loop state trajectories are inside the safety region $\Omega_{\rho_{sp}}$, the objective function reduces to only the average production rate, so the inlet concentration u_1 saturates at its maximum allowable value to increase the reactant concentration x_1, and thus the profit is maximized. The DSLS-LEMPC controller was able to drive the closed-loop state trajectories into the safety region $\Omega_{\rho_{sp}}$ within three sampling periods (i.e., 3Δ). Another

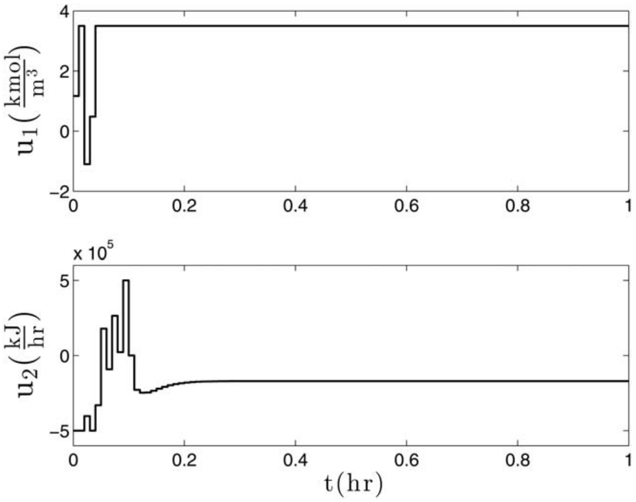

Figure 12. Manipulated input profiles for the closed-loop CSTR under the DSLS-LEMPC design of Eq. 26 for the initial condition $[C_A(0), T(0)]=[1.606\ \frac{kmol}{m^3}, 461.7\ K]$.

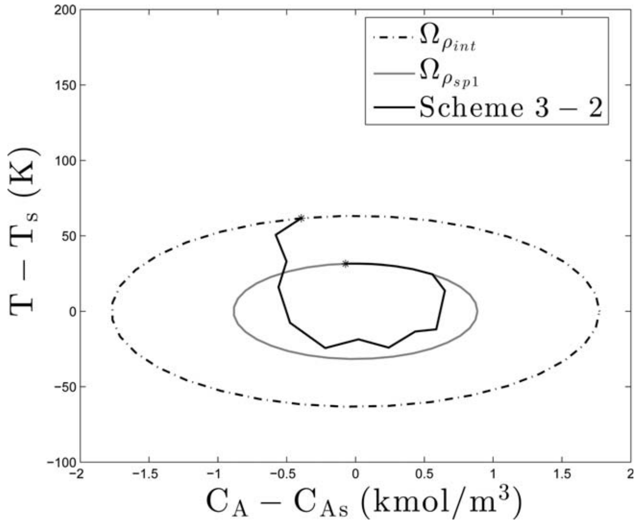

Figure 14. The state-space profile for the closed-loop CSTR under the DSLS-LEMPC design of Eq. 26 for the initial condition $[C_A(0), T(0)]=[1.606\ \frac{kmol}{m^3}, 461.7\ K]$ and $\rho_{int}=2002.3$.

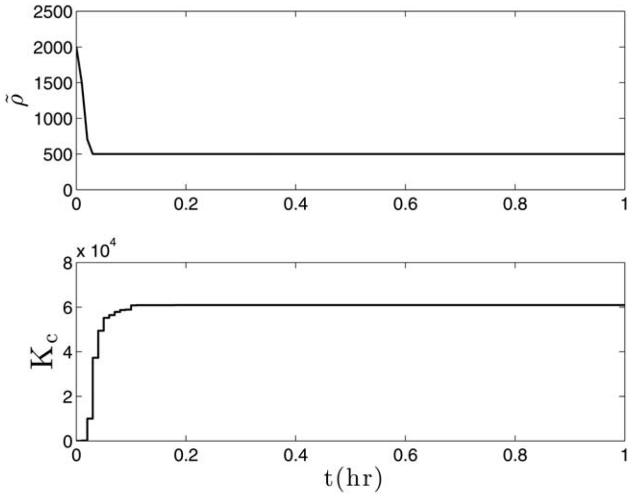

Figure 15. The gain K_c and the initial value of $\tilde{\rho}(t)$ of Eq. 26g at the beginning of each sampling period t_k for the closed-loop CSTR under the DSLS-LEMPC design of Eq. 26 for the initial condition $[C_A(0), T(0)]=[1.606\ \frac{kmol}{m^3}, 461.7\ K]$.

simulation was performed to demonstrate that the DSLS-LEMPC is efficient at adapting to sudden changes of the safety set-point. In this simulation, the safety logic unit required the process state to move to two different safety level sets at two different time instants, where $t_1 = t_0$ and $t_2=0.5\ hr$, with the corresponding safety set-points being $\rho_{sp_1}=500$ and $\rho_{sp_2}=300$. Figure 13 represents the state trajectory in this case; clearly the DSLS-LEMPC was successfully able to drive the closed-loop state into the boundary of $\Omega_{\rho_{sp_2}}$ within one sampling period after t_2 where the process state settled to maximize the profit.

Figure 14 depicts the closed-loop state-space trajectories for x_1 and x_2 starting from an initial level set $\Omega_{\rho_{int}}$ that is equal to the level set Ω_ρ (i.e., $\rho=\rho_{int}=V(x(t_0))$, where t_0 is the initial time). As shown in Figure 14, shortly after the closed-loop state trajectories enter the safety region, they start to approach the boundary of the safety region to maximize the production rate. Also, the state trajectories settle at the point $[x_1(0), x_2(0)]=[0.07\ \frac{kmol}{m^3}, 31.53\ K]$ where the production rate attains a local maximum within the specified safety region $\Omega_{\rho_{sp}}$.

Figure 15 shows the inverse relationship between the gain $K_c(t)$ and the initial value of $\tilde{\rho}(t)$ of Eq. 26g at the beginning of each sampling period t_k under the DSLS-LEMPC design of Eq. 26. The gain $K_c(t)$ levels off at a constant value after the initial value of $\tilde{\rho}(t)$ of Eq. 26g under the DSLS-LEMPC is equal to the safety set-point value $\rho_{sp}=500$.

Remark 29. The formulation of the DSLS-LEMPC used for this example, shown in Eq. 26, is not guaranteed to be stabilizing in the sense of convergence to a small neighborhood of the steady-state, particularly around the unstable steady-state, since it does not include the contractive constraint for simplicity. It was able to maintain the closed-loop state within the stability region in the simulations discussed above; to guarantee convergence to a small neighborhood of the steady-state or robustness to disturbances in this example, the contractive constraint should be added.

Conclusion

In this work, safety-LEMPC schemes were introduced to combine feedback control, process economics, and safety considerations. Three different safety-LEMPC schemes that maintain safe operation while maximizing the profit were developed. The first scheme used a contractive constraint to compute control actions that drive the closed-loop state to a safe region of operation at least as quickly as a stabilizing Lyapunov-based controller would. However, under this scheme, the rate of the transition between the regions of operation may be slow. Although the second scheme utilized a sufficiently long prediction horizon and a region constraint to ensure that the state was within the safety region by a specific time, it may require a long computation time associated with the larger number of decision variables required to simulate a process over a long prediction horizon. The third scheme tackled the drawbacks of the first two schemes by giving two formulations that incorporate time-varying safety-based constraints to transition the closed-loop state between the regions of operation efficiently. The first formulation incorporated a slack variable to achieve this while the second formulation (DSLS-LEMPC) dynamically controlled the upper bound on the Lyapunov function directly. For a sufficiently small sampling period, we proved recursive feasibility and closed-loop stability of a class of nonlinear systems under the safety-LEMPC schemes for nominal operation and, for schemes 1 and 3, in the presence of uncertainty. A chemical process example under each of the safety-LEMPC schemes was presented to demonstrate the ability of the proposed controllers to drive the closed-loop state into a safe region of operation and then maintain it within the safety region while maximizing the profit of the process. Closed-loop stability was maintained in all simulations and the safety-LEMPC schemes demonstrated an effective economic performance and safety constraints satisfaction.

Acknowledgment

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

Literature Cited

1. The 100 largest losses 1972-2011: Large property damage losses in the hydrocarbon industry. Technical report, Marsh & McLennan Companies Inc., 2012.
2. Occupational Safety & Health Administration. OSHA 29 CFR 1910.119. *Process Safety Management of Highly Hazardous Chemicals*.
3. Leveson NG, Stephanopoulos G. A system-theoretic, control-inspired view and approach to process safety. *AIChE J*. 2014;60:2–14.
4. Venkatasubramanian V. Systemic failures: challenges and opportunities in risk management in complex systems. *AIChE J*. 2011;57:2–9.
5. Crowl DA, Louvar JF. *Chemical Process Safety: Fundamentals with Applications*, 3rd ed. Upper Saddle River, NJ: Pearson Education, 2011.
6. Heikkilä A-M, Hurme M, Järveläinen M. Safety considerations in process synthesis. *Comp Chem Eng*. 1996;20:S115–S120.
7. Gentile M, Rogers WJ, Mannan MS. Development of an inherent safety index based on fuzzy logic. *AIChE J*. 2003;49:959–968.
8. Kletz TA. Human problems with computer control. *Plant Operat Prog*. 1982;1:209–211.
9. Leveson NG. *Safeware: System Safety and Computers*. Reading, MA: Addison-Wesley, 1995.
10. Whiteley JR. Potential use of advanced process control for safety purposes during attack of a process plant. *J Hazard Mater*. 2006; 130:42–47.

11. Mhaskar P, El-Farra NH, Christofides PD. Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. *Syst Control Lett.* 2006;55:650–659.
12. Pariyani A, Seider WD, Oktem UG, Soroush M. Incidents investigation and dynamic analysis of large alarm databases in chemical plants: a fluidized-catalytic-cracking unit case study. *Ind Eng Chem Res.* 2010;49:8062–8079.
13. Marlin TE, Hrymak AN. Real-time operations optimization of continuous processes. In *Proceedings of the 5th International Conference on Chemical Process Control*, Vol. 93, pp. 156–164, Tahoe City, CA, 1996.
14. Mayne DQ, Rawlings JB, Rao CV, Scokaert POM. Constrained model predictive control: stability and optimality. *Automatica.* 2000; 36:789–814.
15. Qin SJ, Badgwell TA. A survey of industrial model predictive control technology. *Control Eng Pract.* 2003;11:733–764.
16. Aswani A, Gonzalez H, Sastry SS, Tomlin C. Provably safe and robust learning-based model predictive control. *Automatica.* 2013;49: 1216–1226.
17. Carson JM, Açıkmeşe B, Murray RM, MacMartin DG. A robust model predictive control algorithm augmented with a reactive safety mode. *Automatica.* 2013;49:1251–1260.
18. Angeli D, Amrit R, Rawlings JB. On average performance and stability of economic model predictive control. *IEEE Trans Autom Control.* 2012;57:1615–1626.
19. Ellis M, Durand H, Christofides PD. A tutorial review of economic model predictive control methods. *J Proc Control.* 2014;24:1156–1178.
20. Heidarinejad M, Liu J, Christofides PD. Economic model predictive control of nonlinear process systems using Lyapunov techniques. *AIChE J.* 2012;58:855–870.
21. Huang R, Harinath E, Biegler LT. Lyapunov stability of economically oriented NMPC for cyclic processes. *J Proc Control.* 2011;21: 501–509.
22. Lao L, Ellis M, Durand H, Christofides PD. Real-time preventive sensor maintenance using robust moving horizon estimation and economic model predictive control. *AIChE J.* 2015;61:3374–3389.
23. Lao L, Ellis M, Christofides PD. Smart manufacturing: handling preventive actuator maintenance and economics using model predictive control. *AIChE J.* 2014;60:2179–2196.
24. Khalil HK. *Nonlinear Systems*, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2002.
25. Massera JL. Contributions to stability theory. *Annal Math.* 1956;64: 182–206.
26. Christofides PD, El-Farra NH. *Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-Delays*. Berlin, Germany: Springer-Verlag, 2005.
27. El-Farra NH, Christofides PD. Bounded robust control of constrained multivariable nonlinear processes. *Chem Eng Sci.* 2003;58:3025–3047.
28. Kokotović P, Arcak M. Constructive nonlinear control: a historical perspective. *Automatica.* 2001;37:637–662.
29. Lin Y, Sontag ED. A universal formula for stabilization with bounded controls. *Syst Control Lett.* 1991;16:393–397.
30. Mũnoz de la Peña D, Christofides PD. Lyapunov-based model predictive control of nonlinear systems subject to data losses. *IEEE Trans Autom Control.* 2008;53:2076–2089.
31. Rawlings JB, Amrit R. Optimizing process economic performance using model predictive control. In: Magni L, Raimondo DM, Allgöwer F, editors. *Nonlinear Model Predictive Control: Towards New Challenging Applications*. Berlin, Germany: Springer-Verlag, 2009:119–138.
32. Sontag ED. A 'universal' construction of Artstein's theorem on nonlinear stabilization. *Syst Control Lett.* 1989;13:117–123.
33. Wächter A, Biegler LT. On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. *Math Prog.* 2006;106:25–57.
34. Amrit R, Rawlings JB, Angeli D. Economic optimization using model predictive control with a terminal cost. *Ann Rev Control.* 2011;35:178–186.
35. Mhaskar P, Liu J, Christofides PD. *Fault-Tolerant Process Control: Methods and Applications*. London, England: Springer-Verlag, 2013.

Manuscript received Nov. 29, 2015, and revision received Feb. 17, 2016.