Computers and Chemical Engineering 104 (2017) 76–88

Contents lists available at ScienceDirect

Computers and Chemical Engineering

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

Process operational safety using model predictive control based on a process Safeness Index

Fahad Albalawi[a], Helen Durand[b], Panagiotis D. Christofides[b,a,*]

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

ARTICLE INFO

Article history:
Received 10 February 2017
Received in revised form 14 March 2017
Accepted 6 April 2017
Available online 17 April 2017

Keywords:
Economic model predictive control
Process control
Process safety
Safeness Index
Process operation

ABSTRACT

It has been repeatedly suggested that the common cause-and-effect approach to evaluating process safety has deficiencies that could be addressed by a systems engineering perspective. A systems approach should consider safety as a system-wide property and thus would be required to integrate all aspects of the process involved with monitoring or manipulating the process dynamics, including the control, alarm, and emergency shut-down systems while operating them independently for redundancy. In this work, we propose initial steps in the first systems safety approach that coordinates the control and safety systems through a common metric (a Safeness Index) and develop a controller formulation that incorporates this index. Specifically, this work presents an economic model predictive control (EMPC) scheme that utilizes a Safeness Index function as a hard constraint to define a safe region of operation termed the safety zone. Under the proposed EMPC design, the closed-loop state of a nonlinear process is guaranteed to enter the safety zone in finite time in the presence of uncertainty while maximizing a stage cost that reflects the economics of the process. Closed-loop stability is established for a nonlinear process under the proposed implementation strategy.

1. Introduction

Safety is critical in the chemical process industries due to the severe consequences for both lives and property when safety is not maintained Smith et al. (2003). Despite many efforts to develop, characterize, and standardize effective safe process/plant design and operation procedures, accidents continue to occur causing significant human and capital loss AIChE (1994a,b). There are many causes of these incidents and disasters such as human error, hazardous materials release and manufacturing defects Khan and Abbasi (1999). These consistent accidents throughout chemical process plant history Kidam and Hurme (2013), Kletz (2009) have led some researchers to suggest that the philosophy used in the design of the control and safety system layers (i.e., designing barriers against specific unsafe scenarios using the safety system comprised of the alarms, emergency shut-down, and pressure relief systems as shown in Fig. 1) is quite limited. Particularly, as economic considerations drive more optimized and integrated system designs, a systems approach to analyzing process safety should instead be used (e.g., Leveson and Stephanopoulos (2014), Venkatasubramanian (2011), Mannan et al. (2015), Albalawi et al. (2016)) in which accidents are seen as the result of the process state migrating to an unsafe operating region in state-space over time. Such a viewpoint is radically different from standard industrial thinking, which centers around the notion that the "safeness" of a chemical process increases as barriers such as individual alarms or pressure relief devices are added to the process design for each possible disturbance or equipment fault Crowl and Louvar (2011), Marlin (2012). This traditional philosophy neglects important aspects of the process system, such as multivariable interactions of process variables, limitations on the capacity of process control actuators, and unmonitored process state variables that incorporate valuable process safety information Leveson and Stephanopoulos (2014); accounting for such aspects can be crucial to ensuring process safety.

Some of these issues, such as multivariable interactions and limitations on the capacity of process control actuators, can be accounted for using model predictive control (MPC) Mayne et al. (2000), Rawlings (2000) to regulate the process. The MPC may be augmented with safety-based constraints to handle safety issues (e.g., Albalawi et al. (2017)). Recently, a form of MPC termed Lyapunov-based economic model predictive control (LEMPC) has addressed safety issues by incorporating safety-based constraints and Lyapunov-based constraints within the EMPC to optimize an

[*] Corresponding author.
E-mail address: pdc@seas.ucla.edu (P.D. Christofides).

http://dx.doi.org/10.1016/j.compchemeng.2017.04.010
0098-1354/© 2017 Elsevier Ltd. All rights reserved.

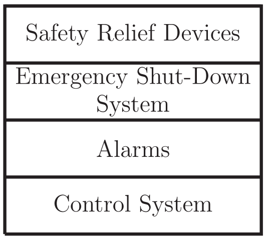

Fig. 1. Control/safety system layers Marlin (2012).

economic measure while ensuring closed-loop stability and process safety (in the sense of maintaining the process state within a Lyapunov level set determined to be a safe operating region in state-space) in the presence of uncertainty Albalawi et al. (2016). However, the assumption that safe operating regions are defined by Lyapunov level sets may be restrictive. Furthermore, addressing safety improvements only at the controller level is not enough to improve process safety overall, because the safety systems at a plant (e.g., alarms, pressure relief devices, and emergency shutdown systems) are often designed without accounting for the impact and limitations of control systems (e.g., they do not account for controller limitations in their triggering thresholds), and they also do not account for multivariable interactions and unmeasured but estimated states of which a model-based control design like MPC can be aware, which can lead to missed alarms at a plant Wang et al. (2016), Ahooyi et al. (2016). Coordinating the process control system with the safety system, while maintaining their independence for redundancy purposes, would represent a significant paradigm shift in both control and safety system design thinking that has the potential to save lives and protect the environment.

The development of a systematic methodology for coordinating safety and control systems poses fundamental challenges; for example, metrics must be developed that can be shared by the control and safety systems to indicate safe or unsafe system operation, and constraints need to be developed for MPC that prevent the closed-loop state from entering unsafe regions based on the developed safety metrics while maintaining closed-loop stability and feasibility. A metric that can unify control and safety systems considerations could improve the designs of both of these systems. Motivated by the above considerations, this work develops a metric termed the Safeness Index that is a function of the closed-loop process state. The terminology Safeness Index indicates the relative safeness of the process state in state-space based on past process data, first-principles models and traditional safety analysis tools. The safety system as well as the control system can then incorporate this index by setting thresholds on the value of this index upon which the actions of the control and safety systems are based. An LEMPC design and implementation strategy that uses the Safeness Index as a hard constraint and maintains closed-loop stability is rigorously developed to demonstrate the incorporation of this metric within a process control system. The proposed Safeness Index framework can be applied to both existing systems and new process systems and technologies. Using a chemical process example, the proposed LEMPC is compared with that of an LEMPC scheme that does not incorporate the Safeness Index-based constraint in terms of its ability to maintain the process state within a region where the value of the Safeness Index is less than a desired threshold.

2. Preliminaries

2.1. Notation

The operator $|\cdot|$ signifies the 2-norm of a vector. The transpose of a vector x is represented by the symbol x^T. The symbol Ω_ρ is used to denote a level set of a continuously differentiable, positive definite scalar-valued function $V(x)$ and is defined by $\Omega_\rho := \{x \in R^n : V(x) \leq \rho\}$. The operator '/' denotes set subtraction, that is, $A/B := \{x \in R^n : x \in A, x \notin B\}$. The symbol $S(\Delta)$ denotes the family of piecewise constant, right-continuous functions with a fixed time interval $\Delta \geq 0$. The initial time instant is denoted by t_0. A function $\alpha(\cdot) : [0, a) \to [0, \infty)$ belongs to class $\mathcal{K}$ if it is strictly increasing and continuous, and $\alpha(0) = 0$.

2.2. Class of nonlinear process systems

The class of nonlinear process systems considered in this work is that of the general form:

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

where $x \in R^n$, $u \in U \subset R^m$, and $w \in R^l$ are the state, input, and disturbance vectors, respectively. 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 $W := \{w \in R^l : |w| \leq \theta, \theta > 0\}$ (i.e., $w(t) \in W$). We assume that the origin is an equilibrium point of the unforced nominal system which implies that $f(0, 0, 0) = 0$.

2.3. Nonlinear system stabilizability assumption

We consider systems of the form of Eq. (1) for which Assumption 1 holds.

Assumption 1. There exists a locally Lipschitz feedback control law $h(x) \in U$ with $h(0) = 0$ for the nominal closed-loop system of Eq. (1) (i.e., $w(t) \equiv 0$) that renders the origin of the closed-loop system with $u = h(x)$ asymptotically stable for all $x \in D \subseteq R^n$ where D is an open neighborhood of the origin, when applied continuously in the sense that there exists Massera (1956), Khalil (2002) a continuously differentiable 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:

$$\begin{aligned} &\alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|) \\ &\frac{\partial V(x)}{\partial x} f(x, h(x), 0) \leq -\alpha_3(|x|) \\ &\left|\frac{\partial V(x)}{\partial x}\right| \leq \alpha_4(|x|) \\ &h(x) \in U, \quad \forall x \in D \subseteq R^n \end{aligned} \tag{2}$$

The stability region of the closed-loop system under the feedback control law that meets Assumption 1 is defined as a level set of the Lyapunov function within D where Eq. (2) holds, and it is denoted by Ω_ρ. Techniques for designing explicit stabilizing control laws for different classes of nonlinear systems can be found in works such as Lin and Sontag (1991), Kokotović and Arcak (2001), El-Farra and Christofides (2003), Christofides and El-Farra (2005).

When x is maintained within the stability region Ω_ρ, we have from the continuity of x, the local Lipschitz property of f, and the continuous differentiability of $V(x)$ that there exist positive constants M, L_x, L_w, L'_x and L'_w such that the following inequalities hold:

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

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

$$\left|\frac{\partial V(x)}{\partial x} f(x, u, w) - \frac{\partial V(x^*)}{\partial x} f(x^*, u, 0)\right| \le L'_x|x - x^*| + L'_w|w| \tag{5}$$

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

When $h(x)$ is applied to the nonlinear process in a sample-and-hold fashion, the following proposition holds.

Proposition 1. *(c.f. Muñoz de la Peña and Christofides (2008), Heidarinejad et al. (2012)) Let Assumption 1 hold, V be the Lyapunov function that satisfies Eq. (2), and Ω_ρ be the resulting stability region. Then if $\rho_s < \rho$, θ, and Δ satisfy*

$$-\alpha_3(\alpha_2^{-1}(\rho_s)) + L'_x M\Delta + L'_w\theta \le -\epsilon_w/\Delta \tag{6}$$

for $\epsilon_w > 0$, then for any $x(t_0) \in \Omega_\rho$,

$$V(x(t)) \le V(x(t_k)), \quad \forall t \in [t_k, t_{k+1}) \tag{7}$$

and

$$V(x(t_{k+1})) < V(x(t_k)) \tag{8}$$

along the closed-loop state trajectory of the sampled-data system

$$\dot{x}(t) = f(x(t), h(x(t_k)), w(t)), \quad \forall t \in [t_k, t_{k+1}), \quad k = 0, 1, \ldots \tag{9}$$

when $x(t_k) \in \Omega_\rho/\Omega_{\rho_s}$. If $\rho_{\min} < \rho$ where

$$\rho_{\min} = \max\{V(x(t + \Delta)) : V(x(t)) \le \rho_s\} \tag{10}$$

then the closed-loop state is always bounded in Ω_ρ and is (uniformly) ultimately bounded in $\Omega_{\rho_{\min}}$ in the sense that:

$$\limsup_{t\to\infty} x(t) \in \Omega_{\rho_{\min}}. \tag{11}$$

$\rho_{\min}$ in the above proposition is defined as the maximum value of the Lyapunov function that will be reached under any sample-and-hold control action (not necessarily $h(x(t_k))$) that meets the input constraints in the presence of bounded disturbances by the end of a sampling time when $x(t_k) \in \Omega_{\rho_s}$.

2.4. Lyapunov-based EMPC

The control design that will be investigated in this work will be a specific type of EMPC termed Lyapunov-based economic model predictive control (LEMPC). LEMPC is a dual-mode optimization-based control strategy that utilizes the Lyapunov-based controller $h(x)$ to define two modes of operation where closed-loop stability is guaranteed in the presence of uncertainty Heidarinejad et al. (2012). The mathematical formulation of LEMPC is as follows:

$$\min_{u \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau)) d\tau \tag{12a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{12b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{12c}$$

$$u(t) \in U, \quad \forall t \in [t_k, t_{k+N}) \tag{12d}$$

$$V(\tilde{x}(t)) \le \rho_e, \forall t \in [t_k, t_{k+N}) \quad \text{if } x(t_k) \in \Omega_{\rho_e} \tag{12e}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \le \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0) \quad \text{if } x(t_k) \notin \Omega_{\rho_e} \tag{12f}$$

where the decision variable of the LEMPC of Eq. (12) is the piecewise constant input trajectory $u(t)$ defined over the prediction horizon $N\Delta$ (i.e., $u \in S(\Delta)$). The optimization problem of Eq. (12) optimizes the economic measure $L_e(x(t), u(t))$ (Eq. (12a)) which defines the cost function, subject to a nominal process model (Eq. (12b)). The initial condition of the nominal process model of Eq. (12b) comes from a measurement of the process state at the current sampling time t_k (Eq. (12c)). Eq. (12d) shows that the calculated control actions $u(t)$ are restricted to the set U over the prediction horizon.

Under the first operation mode (Eq. (12e)), the LEMPC optimizes the economic measure $L_e(x(t), u(t))$ in a time-varying fashion while maintaining the predicted closed-loop state within the set Ω_{ρ_e} which is a subset of the stability region Ω_ρ. The region Ω_{ρ_e} is defined such that if the measured process state at a sampling time t_k is within Ω_{ρ_e}, then at the next sampling time t_{k+1}, it is still within Ω_ρ, even in the presence of bounded disturbances. Under the second operation mode, the LEMPC utilizes a contractive constraint (Eq. (12f)) to ensure that the control action for the first sampling period of the prediction horizon for the closed-loop system forces the state along a path that causes the Lyapunov function value to decrease between two sampling periods. The two-mode operating strategy of LEMPC ensures that the stability region Ω_ρ is a forward invariant set Heidarinejad et al. (2012). The LEMPC produces a set of N input vectors $u^*(t|t_k)$, $t \in [t_k, t_{k+N})$, after solving at each sampling time, but only the input vector $u^*(t_k|t_k)$ corresponding to the first sampling period of the prediction horizon is applied to the process in a sample-and-hold fashion.

Remark 1. The explicit stabilizing controller $h(x)$ provides a feasible control action for both modes of operation of Eq. (12) for $x(t_k) \in \Omega_\rho$. In other words, if the measured state is within Ω_{ρ_e}, then applying $h(\tilde{x}(t_j))$, $\forall t \in [t_j, t_{j+1})$, $j = k, \ldots, k + N - 1$, throughout each corresponding sampling period in the prediction horizon guarantees that the predicted state will be maintained within Ω_{ρ_e} over the prediction horizon (i.e., Eq. (12e) is met by $h(x)$ implemented in sample-and-hold throughout the prediction horizon). If the measured state leaves Ω_{ρ_e}, then applying the explicit stabilizing controller $h(x(t_k))$ for the first sampling period of the prediction horizon, with any other sample-and-hold control action that meets the input constraint of Eq. (12d) throughout the rest of the prediction horizon ($h(\tilde{x}(t_j))$, $\forall t \in [t_j, t_{j+1})$, $j = k + 1, \ldots, k + N - 1$, is a control law that satisfies this requirement by Eq. (2)) is a feasible solution to the LEMPC of Eq. (12) since it meets the contractive constraint of Eq. (12f) applied at the first sampling period of the prediction horizon Heidarinejad et al. (2012).

3. Safeness Index-based control and safety system design

In this section, we develop the concept of a process Safeness Index for use in the control and safety systems. We then discuss techniques that can allow the safety system, as well as the control system, to incorporate this index by setting thresholds on the value of this index that cause the control and safety systems to take certain actions. Finally, we develop a controller that utilizes this index (specifically, the LEMPC scheme of Eq. (12) with a hard constraint related to a threshold on the Safeness Index, termed Safeness Index-based LEMPC) with an implementation strategy that is proven to maintain closed-loop stability of a nonlinear process.

3.1. Development of a process Safeness Index

To effectively integrate the process control and safety systems, it is desirable to develop a Safeness Index that is a function of the process (closed-loop) state only and indicates the safeness of a plant as a whole, given multivariable interactions and interactions between units, which cannot be evaluated with the typical component-by-component safety analyses that are usually performed. Such a state-based index is consistent with the sentiments of various researchers who have stated that a process does not become unsafe automatically, but takes a gradual trajectory in that direction (e.g., Leveson and Stephanopoulos (2014)). The index also benefits from being a function only of the current state; much of the safety thinking in the process industries is a cause-and-effect-type relationship for which the reasons that a state became unsafe are important to the fact that it is unsafe. By developing a Safeness Index that is a function of the current state only, engineers do not need to think of every possible failure mechanism of a system and whether the system is on any of those many paths to understand whether a system is unsafe, but need only characterize where it is on the safeness spectrum based on its present condition. Another benefit of a state-based index is that it can capture safety information even for unmeasured states if an appropriate state estimator is developed, which is not a capability of traditional safety system designs based on process measurements only.

Though the development of a Safeness Index has great promise for improving process safety, the form of the Safeness Index will be process-dependent, and thus a methodology for determining the value of the Safeness Index must be developed. A possible methodology would be to define a function $S(x)$ (the Safeness Index) that can take one of two values at each state-space location (e.g., 0 for 100% safe operating states and 1 for less safe states). An important consideration in the development of a Safeness Index, however, is its intended use in developing constraints in optimization-based control and triggers for the alarm, emergency shut-down, and relief systems, and the binary form of $S(x)$ discussed above would be ineffective for enhancing the safety systems (e.g., the binary function cannot indicate whether the system is near an unsafe state but has not yet reached it, which would be required to trigger elements of the safety system based on $S(x)$ exceeding a threshold). To address these issues, this section develops a systematic methodology for formulating a (not necessarily binary) Safeness Index for a given process based on two factors: (1) $S(x)$ is a function of the process (closed-loop) state only (the path followed to arrive at the state is immaterial; this enables a departure from the limiting cause-and-effect mentality traditionally utilized in chemical process safety system design and accident analysis Leveson (1995), and furthermore, allows the safeness of the system given the controller's effects and limitations to be analyzed); and (2) $S(x)$ indicates the safeness of a plant as a whole, given multivariable interactions and interactions between units, which cannot be evaluated with the component-by-component safety analyses that are usually performed.

The proposed methodology requires analysis, for a given process, of information on past accidents, the results of industrial safety studies, first-principles models, and past operating data to determine both the states that should explicitly appear in $S(x)$ and also a suitable functional dependence of $S(x)$ on these states, as shown in Fig. 2. The first step in this procedure is to determine which states to incorporate in $S(x)$. Initially, an extensive literature review of accidents and their causes (e.g., Kletz (2009), Atherton and Gil (2008), Crowl and Louvar (2011), Khan and Abbasi (1999), Reniers et al. (2013), Tatiya (2011)) can be performed to determine guidelines for states that should be considered based on which states (e.g., temperature, pressure) took abnormal values when past accidents occurred. This study can be used to analyze what kinds of accidents might occur at the plant under consideration, which may have also been investigated for the plant through standard industrial safety analysis techniques (e.g., what-if analyses and HAZOP studies). Any states that are tied to the abnormal situations expected both from the literature review and the safety analyses should be selected for inclusion in $S(x)$. A first-principles model may also reveal that other states should be considered that were perhaps neglected in the qualitative analyses in the early steps due to complexities in the system that are revealed through analyzing the dynamics. For example, it should be checked that $S(x)$: (1) Incorporates states from the model that are known to lead to unsafe/explosive conditions based on the chemistry of the reactions involved (e.g., reactions associated with ignition at certain temperatures Chylla et al. (1987)) or the reactor material limitations (e.g., high temperature or high pressure can lead to reactor rupture); (2) Incorporates states that have a large influence on other states in the reactor that affect process safety; (3) Incorporates all states that influence the safeness of the process, even if these states are unmeasurable or only affect the safeness of the process when they take values far from their values under normal process operating conditions (states that do not indicate the safeness of the process under any condition would not need to be included, however). Analyses like these may be aided through closed-loop simulations of the process from various initial conditions in state-space. Process operating data may also aid in determining which states to incorporate in $S(x)$. For example, process data corresponding to time periods of normal, near-miss (e.g., situations in which the safety system is triggered Pariyani et al. (2010)), and accident operating conditions may be analyzed to determine which states reach values at the near-miss and accident conditions that are significantly different from their values under normal operation, and then include such states in $S(x)$.

After the states to be included in $S(x)$ are identified, it is necessary to determine the functional form of $S(x)$. This functional form should be developed to facilitate the purpose of defining $S(x)$, which is to set thresholds on its value that can be used to distinguish between safe and unsafe operating regions in state-space to cause the control and safety systems to take specific actions based on the threshold values. This indicates that two primary principles should guide the choice of the functional form of $S(x)$: (1) It should be designed so that $S(x)$ will have a significantly larger value when the closed-loop state reaches an unsafe operating region than when it is in a safe operating region; (2) It should incorporate controller limitations and therefore increase rapidly as the boundary of the stability region in which closed-loop stability is guaranteed is approached to reflect that beyond this boundary, the process cannot be guaranteed to be controllable, which is considered an unsafe scenario. Principle 1 may require careful design of $S(x)$ due to potential differences in magnitude of the various states of the process. For example, consider a case in which temperature and concentration of corrosive reactant play a role in the safeness of a chemical process. In many cases, the order of magnitude of the temperature will be greater than that of the concentration, with the result that without careful design of $S(x)$, the reactant concentration may take unsafe values for values of $S(x)$ that are not significantly greater than its value under normal operating conditions or even may be the same as the value of $S(x)$ under normal operating conditions if the temperature drops when the concentration increases. Such a design of $S(x)$ would not facilitate meaningful thresholds being set on its value for use in the control and safety systems; this indicates that scaling of process states or giving $S(x)$ a nonlinear dependence on certain process states may be required when developing the functional form of the Safeness Index. Other cases in which scaling or nonlinearities in $S(x)$ may be beneficial include cases when a process state results in an unsafe condition only when it takes an extreme value, or when the process dynamics are such that there are values of the state vector from which, according to the process dynamics, the state quickly can move from those values to states that pose safety concerns (e.g., if there is a certain pressure P_1 within a reactor from which, under certain conditions, the reactor pressure can quickly elevate to a level that would rupture the reactor, $S(x)$ should become large as this pressure P_1 is reached).

Stability of the closed-loop state can dictate the functional form of the Safeness Index, which allows safety systems that are triggered by a threshold on $S(x)$ to incorporate considerations from the control system in identifying unsafe operating regions. An example of a characterizable form of $S(x)$ that increases as the boundary of the stability region is approached (and, for convenience, is scaled by

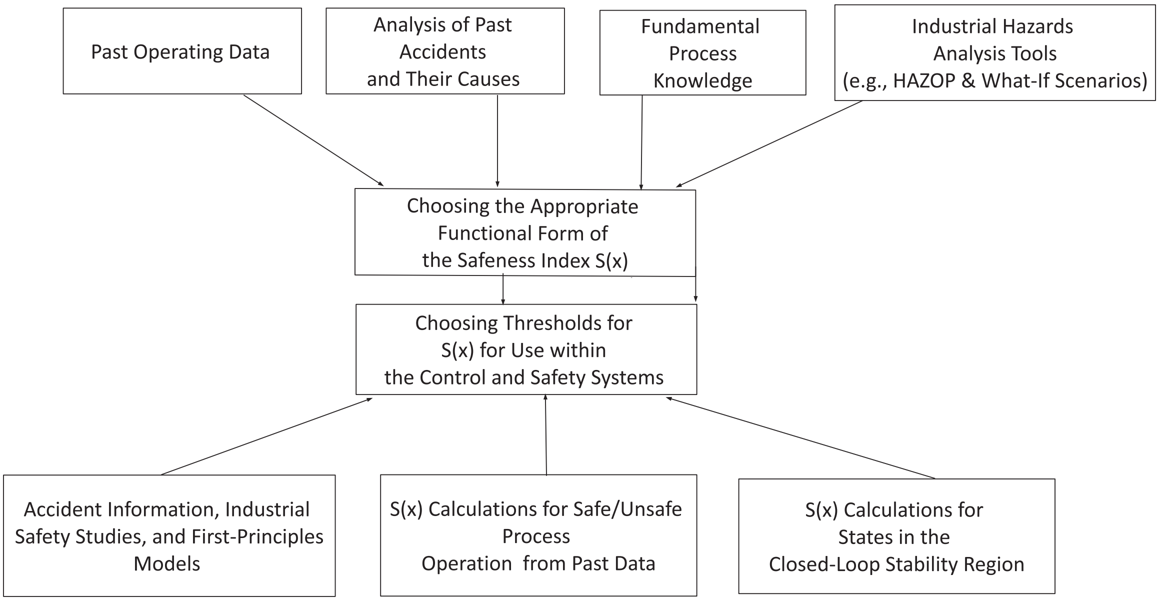
Past Operating Data
Analysis of Past Accidents and Their Causes
Fundamental Process Knowledge
Industrial Hazards Analysis Tools (e.g., HAZOP & What-If Scenarios)
Choosing the Appropriate Functional Form of the Safeness Index S(x)
Choosing Thresholds for S(x) for Use within the Control and Safety Systems
Accident Information, Industrial Safety Studies, and First-Principles Models
S(x) Calculations for Safe/Unsafe Process Operation from Past Data
S(x) Calculations for States in the Closed-Loop Stability Region

Fig. 2. Systematic methodology to construct $S(x)$ and its thresholds.

ρ so that it lies between 0 and 1 and takes a value of 1 on the boundary of the stability region) is a quadratic form (e.g., $S(x)=x^Tx/\rho$). A Safeness Index with a functional form that gives states further from an open-loop unstable operating steady-state a higher value of $S(x)$ may be beneficial if the open-loop trajectories initiated near this steady-state evolve toward an open-loop stable steady-state with a temperature above the allowable operating limits (even when the open-loop unstable steady-state is stabilized by a controller and $S(x)$ is evaluated for the closed-loop state, actuator outputs are typically limited such that beyond a certain region in state-space, the available control energy may no longer prevent the state from reaching unsafe conditions).

3.2. Choosing thresholds for S(x) for use within the control and safety systems

After the functional form of $S(x)$ is determined, it is necessary to set thresholds on $S(x)$ that can be used to modify the control design and trigger the safety system. Fig. 2 illustrates the approach for developing the thresholds on $S(x)$ to be used in the control and safety systems. The control, alarm, emergency shut-down, and relief systems should utilize different thresholds on $S(x)$ for consistency with their independence and also for consistency with standard industrial practice in which the alarms are only activated when the control system does not maintain the process state within a region where all variables instrumented with alarms are within their recommended ranges, and the emergency shut-down system is only activated after another set of thresholds on the instrumented variables is exceeded Marlin (2012). However, because the control system is the first line of defense against unsafe situations (i.e., the safety systems would ideally not be activated frequently for a well-controlled process), the threshold S_{TH} on $S(x)$ utilized by an optimization-based control design should be lower than the thresholds utilized in the safety systems. If the controller then computes control actions subject to a constraint requiring that it should maintain the closed-loop state predictions in a region where the Safeness Index value is less than S_{TH}, false alarms (i.e., activations of the safety system in regions of state-space where the controller guarantees closed-loop stability and guarantees that it can drive the state back into a region where $S(x)<S_{TH}$) may be avoided. Motivated by this, methods for determining S_{TH} will be the focus of this section.

To set the value of S_{TH}, past accidents, the results of industrial safety studies, and first-principles models can be analyzed to gain insight into which values of the states may become large during unsafe conditions and what their expected magnitudes may be to aid in setting S_{TH}. In addition, process data can be valuable for setting S_{TH}. Specifically, past operating data can be labeled as corresponding to safe or unsafe process operating conditions by: (1) labeling the data as "safe" if no alarms were triggered during the time period corresponding to that data set; (2) labeling the data as "safe" if very few (e.g., one or two) alarms sounded during the time period corresponding to the data set, but the closed-loop state subsequently re-entered an operating region where no alarms were triggered without intervention from the operator, emergency shut-down, or relief systems; and (3) labeling data as "unsafe" if a number of alarms sounded during the time period corresponding to that data set. Subsequently, the value of $S(x)$ can be evaluated for each of the labeled data sets. The threshold S_{TH} can then be chosen as a value that is below the minimum value of $S(x)$ observed in the "unsafe" data sets that is significantly different from the values of $S(x)$ observed during "safe" operation to allow "safe" and "unsafe" operating conditions to be appropriately distinguished in the control design. S_{TH} should be somewhat conservatively chosen to allow for other thresholds to be used in triggering the safety system (i.e., the process should not exhibit any negative consequences immediately after $S(x)>S_{TH}$, because that gives the safety system no opportunity to prevent accidents). However, the conservatism in the control design should not be extreme to the point that operating in the region where $S(x)<S_{TH}$ impacts process economics unnecessarily.

Another important consideration in setting S_{TH} for use in an optimization-based control design that utilized stability constraints based on Ω_ρ (e.g., LEMPC) is to ensure that there exist states in the stability region for which $S(x)<S_{TH}$ (if not, there would be no safe operating condition in the region in which the controller ensures closed-loop stability). Therefore, off-line calculations for the value of the Safeness Index $S(x)$ within the stability region Ω_ρ could be performed to validate that with the chosen form of $S(x)$ and the chosen value of S_{TH}, this condition is satisfied. Also, S_{TH} should be set such that when the process is operated in the region where $S(x)<S_{TH}$, none of the thresholds on individual measured variables traditionally utilized to trigger the alarm, emergency shut-down,

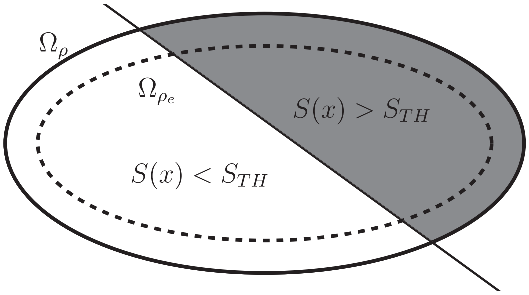

Fig. 3. Example of level set partitioned into "safe" ($S(x) < S_{TH}$), and "unsafe" ($S(x) > S_{TH}$) regions.

or relief systems is surpassed to prevent frequent and unnecessary activation of the safety systems at a plant. The concept of a set of states in state-space being partitioned into "safe" and "unsafe" regions utilizing a threshold on the Safeness Index is illustrated in Fig. 3, where the boundary between the regions occurs at a threshold value $S(x) = S_{TH}$. An illustration of how to define $S(x)$ and S_{TH} will be performed in the context of a chemical process example in Section 4.

Remark 2. The triggering mechanism of the alarm and emergency shut-down systems, and elements of the relief system that can be automated, can be augmented to include not only the traditional triggers based on individual measured variables exceeding or falling below their recommended ranges, but also triggers based on the value of the Safeness Index exceeding threshold values. This can help prevent missed alarms because it allows the safety system to account for multivariable interactions and unmeasured states that may be important in assessing process safety but have traditionally been unavailable to these systems. The thresholds on $S(x)$ utilized by the safety system can come from analyzing industrial safety studies, past accidents, first-principles models, and process operating data as in the evaluation of S_{TH}, except that the thresholds should be tiered so that the thresholds utilized in the alarm, emergency shut-down, and relief systems reflect increasing levels of concern over the process operating conditions. While the control system designs will only use S_{TH} to bound $S(x)$, the various levels of the safety system should be activated by tiered thresholds for consistency with industrial practice. In addition, the threshold value set for the control system should be chosen such that the value of the Safeness Index $S(x)$ of the process state during short excursions from the region where $S(x) \le S_{TH}$ does not reach the threshold value of the alarm system. In other words, the threshold value S_{TH} utilized by the control system should be chosen such that short excursions of the process state outside of the safety zone do not violate the threshold value of the safety system to avoid triggering safety alarms.

Remark 3. $S(x)$ can be defined to take any values within the set of real numbers, but because we consider that the states and inputs are bounded, $S(x)$ will only practically take values within the control system within a subset of the real numbers that correspond to points in state-space where closed-loop stability is guaranteed (i.e., Ω_ρ).

3.3. Safeness Index-based LEMPC formulation

In the remainder of this work, we analyze an optimization-based control design (specifically, an LEMPC) that incorporates a hard constraint requiring that the controller compute control actions that maintain the predicted process state within the region where $S(x) < S_{TH}$. This control design may improve process economic performance and be less conservative than the safety-based control design developed in our prior work Albalawi et al. (2016), where safety-based constraints were included within LEMPC that were triggered when a measurement of the closed-loop state was outside a safe Lyapunov level set of operation termed the safety region $\Omega_{\rho_{sp}} \subset \Omega_\rho$. The level set-based method of triggering safety-based constraints is conceptually the same as developing a binary Safeness Index function that evaluates to either its value corresponding to safe operation within $\Omega_{\rho_{sp}}$ (indicating that the process is within a 100% safe operating region and that the safety-based constraints do not need to be activated) or its value corresponding to unsafe operation outside of $\Omega_{\rho_{sp}}$ (indicating that the process is not operating in a safe region and that the safety-based constraints should be activated). Whenever the process state is within a safe region of operation and the safety-based constraints are not applied, the process economics are optimized while the process state is maintained within this safe region of operation. Thus, process safety is ensured while the process profit is maximized. Despite the guaranteed closed-loop stability and recursive feasibility properties of this method Albalawi et al. (2016), as well as its economic optimization capabilities, it may be unnecessarily restrictive for many processes. For example, regions within which $S(x)$ is below a desired threshold may not be level sets of a Lyapunov function, and trying to find the largest Lyapunov level set within a region where $S(x)$ is less than the threshold may cause the level set to be quite small, which can greatly reduce the economic optimality of process operation within this small region compared to allowing the process to operate within the entire region where $S(x)$ is less than a desired threshold. Furthermore, the threshold value on $S(x)$ may not be a hard threshold (i.e., it may reflect that the process should not in general operate above the threshold, but that short excursions into the region where $S(x)$ is greater than a desired threshold are acceptable; this may be the case, for example, for a reforming tube of a steam methane reformer, for which minor excursions of temperature above the design temperature may reduce the tube lifetime, e.g., increasing the temperature by 20 K can half the lifetime Latham et al. (2011), but will not result in immediate negative consequences). Therefore, allowing $S(x)$ above a threshold value for finite periods of time may be perfectly acceptable from a process safety perspective, and may also be economically beneficial by allowing the closed-loop state to move throughout a larger region of state-space during process operation.

To allow for this less restrictive process operating strategy (for processes for which leaving the region where $S(x)$ is less than a threshold value for finite periods of time is acceptable) while still utilizing LEMPC to allow for economic optimality of process operation, the threshold on the Safeness Index can be used as a hard constraint within LEMPC to form a Safeness Index-based LEMPC design. Specifically, we propose the following formulation of the Safeness Index-based LEMPC:

$$\max_{u(t) \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau)) d\tau \tag{13a}$$

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

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

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

$$\begin{aligned} &V(\tilde{x}(t)) \le \rho_e, \quad \forall t \in [t_k, t_{k+N}) \\ &\text{if} \;\; x(t_k) \in \Omega_{\rho_e} \end{aligned} \tag{13e}$$

$$\begin{aligned} &S(\tilde{x}(t)) \le S_{TH}, \quad \forall t \in [t_k, t_{k+N}) \\ &\text{if} \;\; S(x(t_k)) \le S_{TH} \end{aligned} \tag{13f}$$

$$
\begin{aligned}
&\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \\
&\leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0), \\
&\text{if } \; x(t_k) \in \Omega_\rho / \Omega_{\rho_e} \;\text{ or }\; t_k > t_s \;\text{ or }\; S(x(t_k)) > S_{TH}
\end{aligned}
\tag{13g}
$$

where the notation follows that in Eq. (12). The time t_s is a predetermined time after which it is desired to apply the constraint of Eq. (13g) at each sampling time. The constraint of Eq. (13e) defines the first operation mode of the LEMPC of Eq. (12) and allows the cost function of Eq. (13a) to be maximized while keeping the predicted closed-loop state within Ω_{ρ_e}. When the contractive constraint of Eq. (13g) is not concurrently applied (as it would be if $x(t_k) \in \Omega_{\rho_e}$ but either $t_k > t_s$ or $S(x(t_k)) > S_{TH}$), the constraints of Eqs. (13e)–(13f) allow the controller to enforce a potentially dynamic operating policy to maximize the process economics while maintaining the predicted closed-loop state within the region where $S(\tilde{x}(t)) \leq S_{TH}$ (Eq. (13f)), defined as the safety zone (i.e., the region where the Safeness Index is less than the threshold value for $S(x)$). The hard constraint on the Safeness Index (Eq. (13f)) may also be enforced concurrently with the contractive constraint if the measured state is within the safety zone but either $x(t_k) \in \Omega_\rho / \Omega_{\rho_e}$ or $t_k > t_s$. The role of the contractive constraint is to maintain boundedness of the closed-loop state within the stability region Ω_ρ, and also to drive the closed-loop state back into the safety zone in finite time when it leaves this region when the LEMPC is feasible at every sampling time (an implementation strategy utilizing the LEMPC of Eq. (13) in combination with a Lyapunov-based controller implemented in sample-and-hold is proposed below that is guaranteed to provide closed-loop stability of a nonlinear process within Ω_ρ and to drive the closed-loop state back into the safety zone whenever it exits this region even if the LEMPC is not feasible at every sampling time). Unlike the stability region Ω_ρ, the safety zone is not necessary a forward invariant set because as stated above, the threshold S_{TH} set on the Safeness Index may define a region that is irregularly shaped; for instance, Fig. 3 shows one possible safety zone that is not necessarily a forward invariant set and is irregularly shaped. An important point regarding this formulation is that the origin of the nominal closed-loop system of Eq. (1) is always assumed to be inside the safety zone (i.e., $S(x) \leq S_{TH}$ when $x = 0$).

The fact that the safety zone is not necessarily a forward invariant set means that feasibility of the LEMPC of Eq. (13) cannot be guaranteed whenever the constraint of Eq. (13f) is activated (i.e., whenever $S(x(t_k)) \leq S_{TH}$). This means that though the explicit stabilizing controller $h(\tilde{x}(t_j))$, $\forall t \in [t_j, t_{j+1})$, $j = k, \ldots, k+N-1$, is guaranteed to meet the constraints of Eqs. (13b)–(13e) and the constraint of Eq. (13g) since these constraints form the LEMPC formulation of Eq. (12) (Remark 1) and will thus be a feasible control action whenever $S(x(t_k)) > S_{TH}$, this control law is no longer guaranteed to be feasible when $S(x(t_k)) \leq S_{TH}$. In other words, it is possible that the only feasible control action that satisfies Eqs. (13b)–(13d) and Eqs. (13e) and/or (13g) (depending on whether the conditions that activate Eqs. (13e) and (13g) are active) is $h(x(t_k))$ in the first sampling period with either $h(\tilde{x}(t_j))$, $\forall t \in [t_j, t_{j+1})$, $j = k+1, \ldots, k+N-1$ (if Eq. (13e) is active) or any other control actions that meet Eq. (13c) if Eq. (13e) is not active but Eq. (13g) is (Remark 1). However, controlling a system under $h(x(t_k))$, $\forall t \in [t_k, t_{k+1})$ (and $h(\tilde{x}(t_j))$, $\forall t \in [t_k, t_{k+1})$, $j = k+1, \ldots, k+N-1$) only guarantees that the Lyapunov function of the closed-loop state will decrease between two sampling periods, though it may cause the Lyapunov function to decrease along a path that causes the closed-loop state to leave the safety zone while it decreases the Lyapunov function value. If $h(x(t_k))$, $\forall t \in [t_k, t_{k+1})$ (and $h(\tilde{x}(t_j))$, $\forall t \in [t_j, t_{j+1})$, $j = k+1, \ldots, k+N-1$) is the only feasible solution to the constraints of Eqs. (13b)–(13d) and Eqs. (13e) and/or (13g), but it drives the closed-loop state out of the safety zone, the optimization problem of Eq. (13) becomes infeasible. To deal with this infeasibility issue, we introduce the following implementation strategy for the Safeness Index-based LEMPC that utilizes the solution of the Safeness Index-based LEMPC whenever it is feasible and applies the Lyapunov-based controller in sample-and-hold instead when the LEMPC is infeasible (closed-loop stability of a nonlinear process under this implementation strategy is proven in the next section):

(1) At t_k, a measurement of the current state $x(t_k)$ is received from the sensors; go to Step 2.
(2) Solve the Safeness Index-based LEMPC problem of Eq. (13) and then go to Step 3.
(3) If the Safeness Index-based LEMPC problem of Eq. (13) is feasible, then go to Step 3a. Else, go to Step 3b.
    (a) Apply $u^*(t_k|t_k)$ from the Safeness Index-based LEMPC solution to the nonlinear process in a sample-and-hold fashion, and then go to Step 4.
    (b) Apply the explicit stabilizing controller $h(x)$ in a sample-and-hold fashion (i.e., $u(t) = h(x(t_k))$; $\forall t \in [t_k, t_{k+1})$). Then go to Step 4.
(4) Go to Step 1 ($k \leftarrow k+1$).

Remark 4. It was noted that the Safeness Index-based LEMPC is appropriate for processes for which finite-time excursions of the closed-loop state outside of the safety zone are acceptable from a process safety standpoint (as will be shown in the next section, these excursions of $S(x)$ above S_{TH} do not jeopardize the closed-loop stability of the process because the closed-loop state is always maintained within Ω_ρ under this implementation strategy) and for which there are substantial economic benefits for allowing such excursions. However, for nonlinear processes that cannot tolerate leaving the safety zone, the Safeness Index-based LEMPC can be formulated to handle such processes. In these cases, $S(x)$ can be defined as the Lyapunov function scaled by the value of the Lyapunov function at the boundary of the stability region (i.e., $S(x) = x^T P x/\rho$), and S_{TH} for use within Eq. (13f) can be chosen sufficiently lower than the value of the Lyapunov function corresponding to the actual desired threshold to guarantee closed-loop stability and feasibility within the safety zone even in the presence of disturbances/plant-model mismatch. In this case, the safety zone will be a forward invariant set and closed-loop stability of a nonlinear process initiated within Ω_ρ, guaranteed entry to the safety zone and maintenance of the state within the safety zone after it enters this region, and recursive feasibility of the resulting Safeness Index-based LEMPC would follow from Albalawi et al. (2016), Heidarinejad et al. (2012) if the region where $V(x) \leq S_{TH}$ includes a neighborhood of the origin into which the Lyapunov-based controller implemented in sample-and-hold would drive the closed-loop state. In this case, $h(\tilde{x}(t_j))$, $\forall t \in [t_j, t_{j+1})$, $j = k, \ldots, k+N-1$, would be a feasible solution to the Safeness Index-based LEMPC when the process is initialized within the safety zone.

Remark 5. The fact that $S(x)$ is developed based on the closed-loop state is vital to its effective use within the safety system. Another type of constraint that may be examined as a Safeness Index-based constraint in the context of MPC is a constraint that allows the closed-loop state to increase above a threshold value of $S(x)$ but only for a limited time. This may be the case, for example, for a reforming tube of a steam methane reformer, for which increasing the temperature slightly above the design temperature may decrease tube lifetime but would not be expected to immediately rupture the tube if it had not been in service for long. For this case, the constraint of Eq. (13f) can be replaced with $t_{sum} \leq t_A$ to enforce that the total time t_{sum} in an operating period during which $S(x) > S_{TH}$ be no more than a time length t_A.

Remark 6. In both the Safeness Index-based LEMPC formulation of Eq. (13) and the modification that Remark 5 introduces to the LEMPC formulation of Eq. (13), the value of the Safeness Index for the predicted state trajectory ($S(\tilde{x})$) is constrained to be no greater than the threshold S_{TH} over the prediction horizon $N\Delta$ or to not exceed S_{TH} for more than t_A. However, in some chemical processes the safety of the process is a matter of cumulative behavior of the process state over time; for example, if the temperature of a reactor is above a certain value over some time, that may diminish the material strength of the reactor. In such scenarios, the integration (summation) of the value of $S(x)$ over a given period of time will indicate the safeness of the process. To account for this safety property, the Safeness Index constraint of Eq. (13f) can be replaced with

$$\int_0^t S(x(t\prime))dt\prime \le S_b \tag{14}$$

where S_b is a parameter dependent on the material strength of the process equipment.

Remark 7. In this work, we have focused on the case that a single upper bound S_{TH} is defined on $S(x)$ for use in the control system, though the methodology for the development of thresholds on $S(x)$ and the constraints on $S(x)$ in the control design can be extended to the case that there are both an upper bound and a lower bound on $S(x)$ that indicate the safety of the process (and similarly in the safety system).

Remark 8. The discussion in this section shows that another consideration for setting S_{TH} is the control system design that will incorporate this threshold. Because $S(x)$ may exceed S_{TH} under the Safeness Index-based LEMPC design (though the state will always be driven back into the safety zone), the threshold S_{TH} may be more conservatively chosen when such a control design is used. If, as in Remark 4, $S(x)$ is a Lyapunov function, the region in which it is desired to maintain the closed-loop state for safety reasons may be more directly tied to the values of the process states as the state approaches unsafe conditions because the controller can guarantee that the state will not leave the region where $S(x)$ is below a desired value. Also, to guarantee closed-loop stability under the implementation strategy of the control design presented in this section (which will be shown in the next section), the safety zone has to be defined to include $\Omega_{\rho_{\min}}$, which affects both the form of $S(x)$ and its thresholds.

3.4. Feasibility and stability analysis

In this subsection, we present sufficient conditions to show that the state of the closed-loop system of Eq. (1) under the Safeness Index-based LEMPC implementation strategy is guaranteed to enter the safety zone where $S(x) \le S_{TH}$ in finite time and to remain within the stability region Ω_ρ at all times. Moreover, we prove that the closed-loop state is guaranteed to be ultimately bounded in a small region containing the origin. To proceed, we first re-state two propositions from Heidarinejad et al. (2012) to define functions and parameters needed for the proof of closed-loop stability of a nonlinear process the Safeness Index-based LEMPC implementation strategy, and then present Theorem 1 that gives sufficient conditions for the proof of closed-loop stability of a nonlinear process under the Safeness Index-based LEMPC implementation strategy.

Proposition 2 (c.f. Heidarinejad et al. (2012), Mhaskar et al. (2013)). *Consider the systems*

$$\begin{aligned}\dot{x}_a(t) &= f(x_a(t), u(t), w(t)) \\ \dot{x}_b(t) &= f(x_b(t), u(t), 0)\end{aligned} \tag{15}$$

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

$$|x_a(t) - x_b(t)| \le f_W(t - t_0), \tag{16}$$

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

$$f_W(\tau) = \frac{L_w\theta}{L_x}(e^{L_x\tau} - 1). \tag{17}$$

Proposition 3 (c.f. Heidarinejad et al. (2012), Mhaskar et al. (2013)). *Consider the Lyapunov function $V(\cdot)$ of the system of Eq. (1). There exists a quadratic function $f_V(\cdot)$ such that*

$$V(x) \le V(\hat{x}) + f_V(|x - \hat{x}|) \tag{18}$$

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

$$f_V(s) = \alpha_4(\alpha_1^{-1}(\rho))s + M_v s^2 \tag{19}$$

where M_v is a positive constant.

Theorem 1. *Consider the system of Eq. (1) in closed-loop under the implementation strategy (Steps 1–4) of the Safeness Index-based LEMPC of Eq. (13) based on a controller $h(x)$ that satisfies the conditions of Eq. (2). Let $\epsilon_w > 0$, $\Delta > 0$, $\rho > \rho_e > \rho_s > 0$ satisfy*

$$\rho_e \le \rho - f_V(f_W(\Delta)) \tag{20}$$

and

$$-\alpha_3(\alpha_2^{-1}(\rho_s)) + L\prime_x M\Delta + L\prime_w\theta \le -\epsilon_w/\Delta. \tag{21}$$

If $x(t_0) \in \Omega_\rho$, $\rho_{\min} \le \rho$ and $N \ge 1$ where $\rho_{\min}$ is defined as in Eq. (10) and where the compact set $\Omega_{\rho_{\min}}$ satisfies

$$\Omega_{\rho_{\min}} \subseteq \{x \in \Omega_\rho : S(x) \le S_{TH}\}, \tag{22}$$

then the closed-loop state $x(t)$ of Eq. (1) is guaranteed to enter the safety zone in finite time when $x(t_0) \in \Omega_\rho$, to be bounded within Ω_ρ at all times, and to be ultimately bounded in $\Omega_{\rho_{\min}}$.

Proof. The proof consists of two parts. The first part is the proof that an input trajectory with characterizable properties exists for a nonlinear process operated under Steps 1–4 of the Safeness Index-based LEMPC implementation strategy when $x(t_0) \in \Omega_\rho$. The second part is the proof of the three results of Theorem 1 given these characterizable properties.

Part 1: To prove the results of Theorem 1, it is necessary to prove that the inputs applied to the process from the Safeness Index-based LEMPC implementation strategy are characterizable so that closed-loop stability of a nonlinear process under such input trajectories can be investigated. According to the implementation strategy, in a given sampling period, one of two cases will occur: (1) the Safeness Index-based LEMPC of Eq. (13) is a feasible optimization problem and $u^*(t_k|t_k)$ is applied to the process for $t \in [t_k, t_{k+1})$; (2) the Safeness Index-based LEMPC of Eq. (13) is not a feasible optimization problem and $h(x(t_k))$ is applied for $t \in [t_k, t_{k+1})$. In the first case when the Safeness Index-based LEMPC is feasible, this means that a feasible solution was determined that satisfied the constraints of Eqs. (13b)–(13g) for the nominal closed-loop system for the given sampling period. In the second case when the LEMPC is not feasible and $h(x)$ is applied in a sample-and-hold fashion, the conditions of Proposition 1 hold for the given sampling period. Thus, for any given sampling period, the conditions met by the control actions that are implemented can be characterized, and therefore the conditions met by the input trajectory applied throughout time can be characterized and thus used in analyzing closed-loop stability.

Part 2: We now prove the results of Theorem 1. Specifically, we prove that if the closed-loop state of the nonlinear process under the Safeness Index-based LEMPC implementation strategy is initialized within the stability region Ω_ρ, even outside the safety zone (i.e., $S(x(t_0)) > S_{TH}$), then within finite time the closed-loop state will enter the safety zone. Furthermore, we prove that for any $x(t_0) \in \Omega_\rho$, the closed-loop state remains within the stability region Ω_ρ at all times. We also show that if $t_k > t_s$, then the closed-loop state will be ultimately bounded in a compact set containing the origin.

To prove that the closed-loop state will always enter the safety zone in finite time under the Safeness Index-based LEMPC implementation strategy when it is either initiated outside of this region or leaves this region while operated in closed-loop when the process is initiated from any initial condition $x(t_0) \in \Omega_\rho$, we first show that the closed-loop state under either a feasible solution to the Safeness Index-based LEMPC of Eq. (13) or under $h(x)$ implemented in sample-and-hold will drive the closed-loop state toward the set $\Omega_{\rho_{\min}}$ throughout a given sampling period, where $\Omega_{\rho_{\min}}$ is within the safety zone from Eq. (22). When $S(x(t_k)) > S_{TH}$ and the Safeness Index-based LEMPC is feasible at t_k, the contractive constraint of Eq. (13g) is active. In Heidarinejad et al. (2012), it is proven that when the conditions of Eqs. (20)–(21) are satisfied, $V(x(t)) \leq V(x(t_k))$, $\forall\, t \in [t_k, t_{k+1})$, and $V(x(t_{k+1})) < V(x(t_k))$ along the trajectories of the closed-loop system under an LEMPC containing the contractive constraint, even in the presence of bounded disturbances, when $x(t_k) \notin \Omega_{\rho_s} \subseteq \Omega_{\rho_{\min}}$. If the Safeness Index-based LEMPC is infeasible at t_k, $h(x(t_k))$ is applied, which causes Eqs. (7)–(8) to hold when $x(t_k) \notin \Omega_{\rho_s} \subseteq \Omega_{\rho_{\min}}$. This means that in a given sampling period, whether $u^*(t_k|t_k)$ is applied or $h(x(t_k))$ according to the implementation strategy, the Lyapunov function value of the closed-loop state is guaranteed to decrease throughout the sampling period. At each sampling time until $S(x(t_k)) \leq S_{TH}$, the contractive constraint of Eq. (13g) will remain active and therefore the Lyapunov function value will continue to decrease. Therefore, the closed-loop state will either enter the safety zone in finite time (before it enters $\Omega_{\rho_{\min}}$), or Eq. (13g) will continue to be applied within the LEMPC and the Safeness Index-based LEMPC implementation strategy will continue to cause $V(x(t)) \leq V(x(t_k))$, $\forall\, t \in [t_k, t_{k+1})$, until the closed-loop state enters $\Omega_{\rho_{\min}}$. Because Eq. (22) holds, and the closed-loop state enters $\Omega_{\rho_{\min}}$ in finite time from any initial condition in Ω_ρ, the closed-loop state is thus guaranteed to enter the safety zone, regardless of its shape, within finite time, from any $x(t_k) \in \Omega_\rho$ where $S(x(t_k)) > S_{TH}$, even in the presence of disturbances.

To prove that Ω_ρ is a forward invariant set under the Safeness Index-based LEMPC implementation strategy (i.e., when $x(t_0) \in \Omega_\rho$, $x(t) \in \Omega_\rho\ \forall\, t \in [t_0, \infty)$), we first demonstrate that in a given sampling period, if $x(t_k) \in \Omega_\rho$, then $x(t_{k+1}) \in \Omega_\rho$ both in the case that the Safeness Index-based LEMPC of Eq. (13) has a feasible solution throughout the prediction horizon $N\Delta$, and in the case that it does not and $h(x(t_k))$ is applied for $t \in [t_k, t_{k+1})$. When the Safeness Index-based LEMPC is feasible, the stability results of Heidarinejad et al. (2012) hold because they are based only on feasibility of the Lyapunov-based stability constraints of Eqs. (13e) and (13g) and do not depend on whether other constraints such as Eq. (13f) are enforced. Specifically, if $x(t_k) \in \Omega_{\rho_e}$ such that the constraint of Eq. (13e) is active, then $\tilde{x}(t_{k+1}) \in \Omega_{\rho_e}$ and $x(t_{k+1}) \in \Omega_\rho$ from the constraint of Eq. (13e), Propositions 2–3, and Eq. (20). If $x(t_k) \in \Omega_\rho / \Omega_{\rho_e}$, then Eq. (13g) is active, which decreases the Lyapunov function value between two sampling periods and thus ensures that the closed-loop state enters a lower level set (and thus cannot exit Ω_ρ). When the Safeness Index-based LEMPC has no feasible solution throughout the prediction horizon, then $h(x(t_k))$ will be applied between two sampling times, which will decrease the Lyapunov function between the two sampling times and thus ensure that the closed-loop state does not leave Ω_ρ in that sampling period. If $x(t_0) \in \Omega_\rho$, then recursive application of the property that $x(t_k) \in \Omega_\rho$ ensures that $x(t_{k+1}) \in \Omega_\rho$, starting with $k = 0$, shows that the Safeness Index-based LEMPC implementation strategy maintains the closed-loop state within Ω_ρ at all times.

To prove that if $t_k > t_s$, the closed-loop state under the Safeness Index-based LEMPC implementation strategy is ultimately bounded in $\Omega_{\rho_{\min}}$, we note that under this condition, the contractive constraint of Eq. (13g) will be active within the LEMPC, and either the LEMPC will be feasible or $h(x(t_k))$ will be applied to the process throughout the sampling period. As noted above, control actions generated from either the LEMPC or from $h(x(t_k))$ under this condition will continue to decrease the Lyapunov function value until the closed-loop state enters the compact set $\Omega_{\rho_{\min}}$ in a finite time. From the definition of $\Omega_{\rho_{\min}}$, once the closed-loop state enters $\Omega_{\rho_{\min}}$, if $u^*(t_k|t_k)$ that meets the contractive constraint or $h(x(t_k))$ is then applied to the process, decreasing the Lyapunov function value until the closed-loop state enters Ω_{ρ_s}, the closed-loop state cannot leave $\Omega_{\rho_{\min}}$. The proof of this is analogous to the proof of ultimate boundedness in Heidarinejad et al. (2012). □

Remark 9. It is noted that if Eq. (22) holds, then if $t_k > t_s$ and the closed-loop state has entered $\Omega_{\rho_{\min}}$ and is ultimately bounded there, the closed-loop state is within the safety zone for all subsequent times. This shows that if it is found that the closed-loop state under the Safeness Index-based LEMPC implementation strategy is spending an undesirable length of time above the safety threshold, the current sampling time t_k can be set to t_s to cause the Safeness Index-based LEMPC implementation strategy to drive the closed-loop state into a region where the threshold on the Safeness Index is always met and to maintain closed-loop operation in this region until the value of S_{TH} can be redesigned so that the Safeness Index-based LEMPC causes the closed-loop state to remain below a desired threshold for more of the operating time.

4. Application to a chemical process example

In this section, a chemical process example is provided to illustrate the ability of the Safeness Index-based LEMPC to maintain the closed-loop state within a region where $S(x(t_k)) \leq S_{TH}$ when the LEMPC of Eq. (12) would not compute an input trajectory that achieves this. The chemical process example is a well-mixed, non-isothermal continuous stirred tank reactor (CSTR) where an irreversible second-order exothermic reaction takes place. The reaction transforms a reactant A to a product B ($A \rightarrow B$). The feedstock of the CSTR consists of pure A and the inlet concentration of A is C_{A0}. The inlet temperature and feed volumetric flow rate of the reactor are T_0 and F, respectively. The CSTR is equipped with a heating jacket that heats/cools the reactor at a heat rate Q. The process has two states, C_A for the concentration of the reactant species A and T for the reactor temperature, and these states are taken to evolve according to the mass and energy balances derived from first-principles modeling of the CSTR with standard chemical engineering assumptions as follows:

$$\frac{dC_A}{dt} = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{R_g T}} C_A^2 \tag{23a}$$

$$\frac{dT}{dt} = \frac{F}{V}(T_0 - T) + \frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{R_g T}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{23b}$$

The notation ΔH, k_0, E, and R_g represent the enthalpy of reaction, pre-exponential constant, activation energy, and ideal gas constant, respectively. The reactor volume V, heat capacity C_p, and fluid density ρ_L within the reactor are assumed constant (process parameter values are listed in Table 1). The dynamic model of Eq. (23) is integrated numerically by using the explicit Euler method with an integration time step of $h_c = 10^{-5}$ h.

The manipulated inputs are the concentration C_{A0} of the reactant species A in the feed and the heat input/removal rate Q. The process of Eq. (23) has three steady-states with associated steady-state input values $[C_{A0s} \;\; Q_s] = \left[4\,\frac{\text{kmol}}{\text{m}^3} \;\; 0\,\frac{\text{kJ}}{\text{h}}\right]$. The CSTR is operated around an open-loop asymptotically stable steady-state that occurs

Table 1
Parameter values.

$T_0 = 300$	K	$F = 5$	$\frac{\mathrm{m}^3}{\mathrm{h}}$
$V = 1.0$	m^3	$E = 5 \times 10^4$	$\frac{\mathrm{kJ}}{\mathrm{kmol}}$
$k_0 = 8.46 \times 10^6$	$\frac{\mathrm{m}^3}{\mathrm{kmolh}}$	$\Delta H = -1.15 \times 10^4$	$\frac{\mathrm{kJ}}{\mathrm{kmol}}$
$C_p = 0.231$	$\frac{\mathrm{kJ}}{\mathrm{kgK}}$	$R = 8.314$	$\frac{\mathrm{kJ}}{\mathrm{kmolK}}$
$\rho_L = 1000$	$\frac{\mathrm{kg}}{\mathrm{m}^3}$	$C_{As} = 1.2$	$\frac{\mathrm{kmol}}{\mathrm{m}^3}$
$T_s = 438$	K	$C_{A0s} = 4$	$\frac{\mathrm{kmol}}{\mathrm{m}^3}$
$Q_s = 0$	$\frac{\mathrm{kJ}}{\mathrm{h}}$		

at $[C_{As} \quad T_s] = \left[1.2\,\frac{\mathrm{kmol}}{\mathrm{m}^3} \quad 438\,\mathrm{K}\right]$. The dynamic model of Eq. (23) is in the following class of nonlinear systems:

$$\dot{x}(t) = \tilde{f}(x(t)) + g_1(x(t))u_1(t) + g_2(x(t))u_2(t) \tag{24}$$

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

$$L_e(x, u) = \frac{k_0 e^{-\frac{E}{R_g T}} C_A^2}{N\Delta} \tag{25}$$

where the prediction horizon $N = 10$ and the sampling period $\Delta = 0.01$ h. In addition, a material constraint that represents the limitation on the amount of reactant material available over a given operating period $t_p = 1.0$ h is described by the following constraint:

$$\frac{1}{t_p} \int_0^{t_p} u_1(\tau) d\tau = 0.0\,\mathrm{kmol/m}^3. \tag{26}$$

The Safeness Index function $S(x)$ for the CSTR is designed as follows so that points in state-space with higher temperatures have larger values of $S(x)$:

$$S(x) = \frac{ax_1 + bx_2}{\max\{ax_1 + bx_2 : V(x) \leq \rho\}} \tag{27}$$

where a and b are weighting constants. The value of the Safeness Index $S(x)$ of Eq. (27) varies between −1 and 1, where −1 indicates the safest point at which to operate in state-space and 1 indicates the most unsafe point at which to operate in state-space within the stability region Ω_ρ. In the simulation below, the weighting constants a and b are set to 1 so that the deviation variable form of the temperature (x_2), which can reach several orders of magnitude above the deviation form of C_A (x_1), contributes heavily to the value of the Safeness Index $S(x)$ at a given state. The maximum value of $\max\{ax_1 + bx_2 : V(x) \leq \rho\}$ within the stability region is 74.46. The Safeness Index threshold value S_{TH} is set to 0.6 so that the reactor temperature in deviation form from the steady-state value cannot exceed 47 K (i.e., $x_2 \leq 47$ K). To guarantee closed-loop stability of the process considered under the controller of Eq. (13), a Lyapunov-based controller of the form $h(x) = [h_1(x)\, h_2(x)]^T$ is constructed to estimate the stability region for the Safeness Index-based LEMPC. The inlet concentration control law $h_1(x)$ is set to its steady-state value ($h_1(x) = 0.0\,\mathrm{kmol/m}^3$) so that the material constraint of Eq. (26) is met. The following feedback law (Sontag control law Lin and Sontag (1991)) is utilized for the heat rate u_2:

$$h_2(x) = \begin{cases} -\dfrac{L_{\tilde{f}}V + \sqrt{L_{\tilde{f}}V^2 + L_{g_2}V^4}}{L_{g_2}V}, & \text{if } \; L_{g_2}V \neq 0 \\ 0, & \text{if } \; L_{g_2}V = 0 \end{cases} \tag{28}$$

where $L_{\tilde{f}}V$ and $L_{g_2}V$ are the Lie derivatives of the Lyapunov function $V(x)$ with respect to the vector fields $\tilde{f}(x)$ and $g_2(x)$ respectively. The control law of Eq. (28) is subject to the input constraint (i.e., $|h_2(x)| \leq 5 \times 10^5\,\frac{\mathrm{kJ}}{\mathrm{h}}$). Extensive closed-loop simulations were performed under the Lyapunov-based controller $h(x)$ to construct the regions needed in designing stability constraints in the LEMPC of Eq. (12). A quadratic Lyapunov function of the form $V(x) = x^T P x$ was utilized to estimate the stability region of the closed-loop system with the following positive definite P matrix:

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

Using this Lyapunov function, ρ was chosen to be 368 and ρ_e was chosen to be 340.

To show that the Safeness Index-based LEMPC is capable of maintaining closed-loop operation within the region where $S(x) \leq S_{TH}$, even when the LEMPC of Eq. (12) without the Safeness Index-based constraint would not achieve this, we apply both controllers to the CSTR of Eq. (23), where the two optimization problems at each sampling time were solved using the interior-point solver Ipopt Wächter and Biegler (2006). The CSTR was initiated in both cases from the steady-state ($x_{\mathrm{int}}^T = \left[0\,\frac{\mathrm{kmol}}{\mathrm{m}^3} \quad 0\,\mathrm{K}\right]$) where the Safeness Index $S(x)$ equals zero.

Fig. 4 shows the closed-loop input trajectories for the CSTR under the Safeness Index-based LEMPC scheme and the LEMPC scheme of Eq. (12) throughout one hour of operation. The input met the material constraint of Eq. (26) under both controllers. Also, the heat rate u_2 of both schemes settled at its steady-state value $u_2 = 0\,\frac{\mathrm{kJ}}{\mathrm{h}}$ for close to eighty percent of the one hour of operation, and then deviated from its steady-state value at the end of the simulation so that the other constraints of the formulation (e.g., the material constraint) could be met by the controller while continuing to optimize process economics. Fig. 5 depicts the trajectories of the reactant concentration and reactor temperature in deviation from the steady-state values ($[x_1 \; x_2] = [C_A - C_{As} \; T - T_s]$). From Figs. 4 and 5, it is seen that before the end of the simulation, the behavior of the closed-loop state and the input trajectories under both the Safeness Index-based LEMPC scheme and the LEMPC scheme of Eq. (12) are overlapping. This overlap is contributed to by the goal of both LEMPC's to maximize the production rate of B within the stability region over the prediction horizon, which is achieved

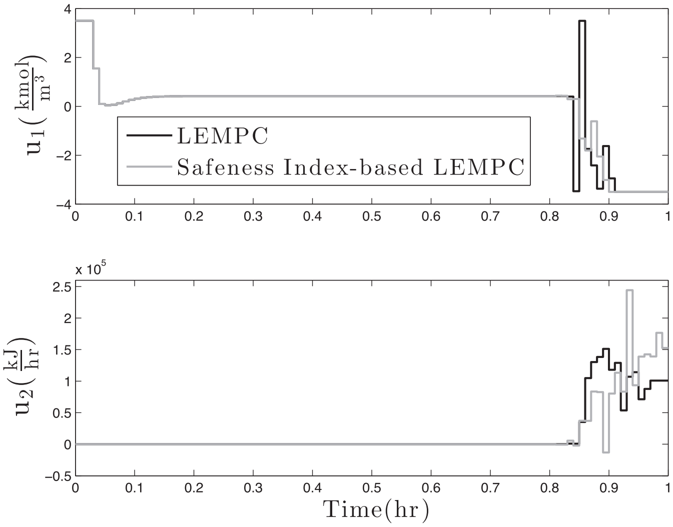

Fig. 4. Manipulated input profiles for the closed-loop CSTR under the LEMPC design of Eq. (12) and under the Safeness Index-based LEMPC design of Eq. (13) for the initial condition $x_{\mathrm{int}}^T = \left[0\,\frac{\mathrm{kmol}}{\mathrm{m}^3} \quad 0\,\mathrm{K}\right]$.

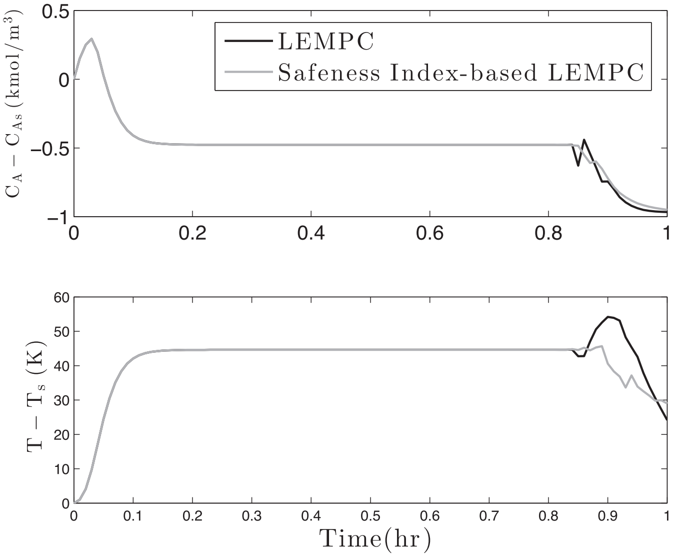

Fig. 5. The state profiles for the closed-loop CSTR under the LEMPC design of Eq. (12) and under the Safeness Index-based LEMPC design of Eq. (13) for the initial condition $x_{\text{int}}^T = \left[0\ \frac{\text{kmol}}{\text{m}^3}\ \ 0\,\text{K}\right]$.

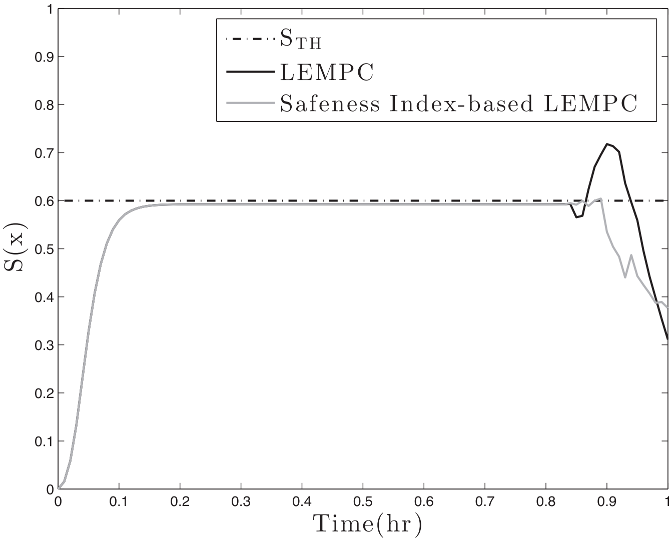

Fig. 6. The Safeness Index function $S(x)$ for the closed-loop CSTR under the LEMPC design of Eq. (12) and under the Safeness Index-based LEMPC design of Eq. (13) for the initial condition $x_{\text{int}}^T = \left[0\ \frac{\text{kmol}}{\text{m}^3}\ \ 0\,\text{K}\right]$.

under both LEMPC's for much of the period of operation by maintaining the closed-loop state at $[x_1\ \ x_2] = \left[-0.477\ \frac{\text{kmol}}{\text{m}^3}\ \ 44.6\,\text{K}\right]$, which is within the safety zone (i.e., $S(x) = 0.59 \leq 0.6$ where $x = \left[-0.477\ \frac{\text{kmol}}{\text{m}^3}\ \ 44.6\,\text{K}\right]$). At the end of the simulation, the LEMPC's ensure that the material constraint of Eq. (26) is met before the end of the operating period. When the constraint on $S(x)$ is not imposed, the LEMPC of Eq. (12) computes a solution that maximizes the process economics, but leaves the safety region; therefore, the Safeness Index-based LEMPC computes a different trajectory than the LEMPC of Eq. (12) at the end of the prediction horizon that meets the material constraint and also maximizes the process economics but subject to the requirement that the closed-loop state cannot leave the safety region. Specifically, Fig. 5 shows that the closed-loop trajectory of the reactor temperature under the Safeness Index-based LEMPC decreases, while that under the LEMPC design of Eq. (12) exceeds the maximum temperature set by the Safeness Index function $S(x)$ because it lacks the Safeness Index-based constraints.

Fig. 6 further demonstrates that the LEMPC of Eq. (12) causes S_{TH} to be exceeded at the end of the operating window by presenting the Safeness Index value $S(x)$ for the LEMPC of Eq. (12) and the Safeness Index-based LEMPC over the operating window. Fig. 7, which displays the state-space trajectories of the reactant concentration and reactor temperature in deviations from the steady-state values ($[x_1\ x_2] = [C_A - C_{As}\ T - T_s]$), also shows this. The closed-loop trajectory under the LEMPC of Eq. (12) is seen to leave the safety zone (shaded gray), whereas the closed-loop state under the Safeness Index-based LEMPC never leaves the safety zone.

To illustrate the robustness of the Safeness Index-based LEMPC of Eq. (13) and the LEMPC of Eq. (12), a bounded disturbance vector $w^T = [w_1 w_2]$ was added to the right-hand side of Eq. (23). The bounded disturbance vector $w^T = [w_1 w_2]$ corresponds to Gaussian white noise with variances $\sigma_1 = 1\ \frac{\text{kmol}}{\text{m}^3}$ and $\sigma_2 = 20\,\text{K}$ with $|w_1| \leq 1\ \frac{\text{kmol}}{\text{m}^3}$ and $|w_2| \leq 20\,\text{K}$. Figs. 8 and 9 show the corresponding manipulated input and state profiles starting from the same initial condition but under bounded process disturbances for both schemes. In the presence of disturbances, the inlet concentration u_1 satisfied the material constraint of Eq. (26) under the Safeness Index-based LEMPC and the LEMPC of Eq. (12). The heating rate u_2 exhibited similar closed-loop behavior as the case of nominal operation for the Safeness Index-based LEMPC, while u_2 exhibited different closed-loop behavior for the LEMPC in the presence of disturbances. Unlike the case of nominal operation, the closed-loop trajectory of the reactor temperature under the LEMPC exceeds the maximum allowable temperature 47 K for almost half of the operating window due to the disturbance. Figs. 10 and 11 demonstrate that the Safeness Index-based LEMPC was able to maintain the closed-loop state within the safety zone at all times even in the presence of uncertainty while the closed-loop state trajectory under the LEMPC of Eq. (12) left the safety zone and never went back to it. It is noted that the two simulations under the different controllers in Figs. 8–11 had different realizations of the process disturbance than each other at each sampling time (though with the same bounds and standard deviation for the disturbance distribution), which has also contributed to the differences in the trajectories presented.

Remark 10. In the above simulation results, for both nominal process operation (i.e., $w = 0$) and in the presence of disturbance,

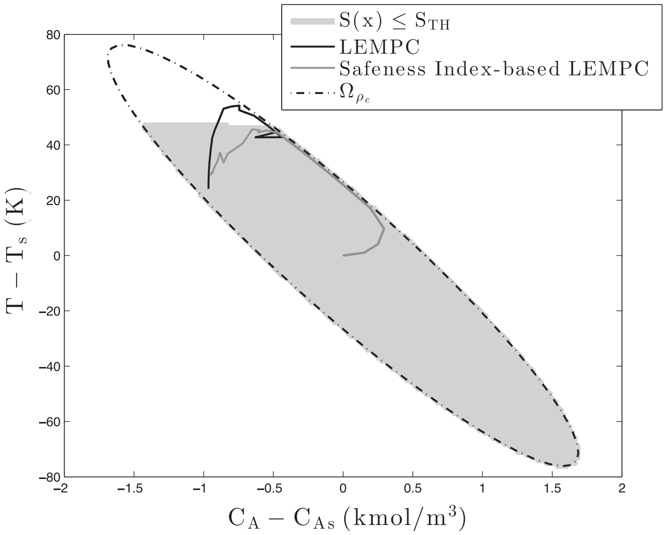

Fig. 7. The state-space profile for the closed-loop CSTR under the LEMPC design of Eq. (12) (black trajectory) and under the Safeness Index-based LEMPC design of Eq. (13) (dark gray trajectory) for the initial condition $x_{\text{int}}^T = \left[0\ \frac{\text{kmol}}{\text{m}^3}\ \ 0\,\text{K}\right]$.

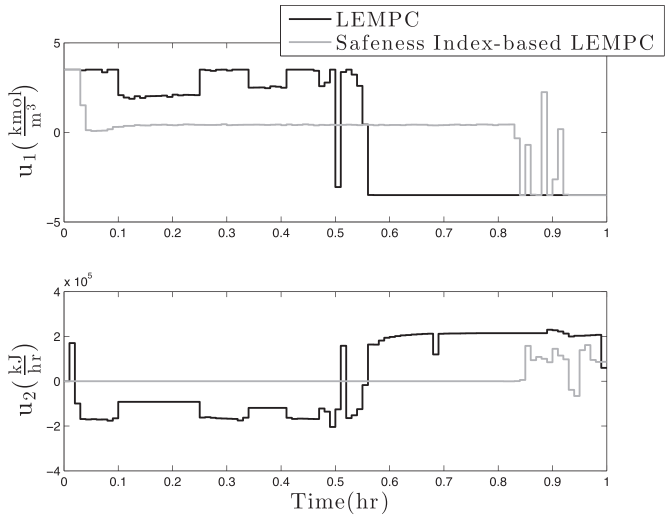

Fig. 8. Manipulated input profiles for the closed-loop CSTR under the LEMPC design of Eq. (12) and under the Safeness Index-based LEMPC design of Eq. (13) for the initial condition $x_{int}^T = \left[0\ \frac{kmol}{m^3}\quad 0\,K\right]$ with bounded process disturbances.

the Safeness Index-based LEMPC of Eq. (13) was feasible at each sampling time when different values of the upper bound of the disturbance were considered. However, in the presence of disturbances that have certain upper bound values (e.g., $\theta_1 = 1\ \frac{kmol}{m^3}$ and $\theta_2 = 40\,K$), the classical LEMPC was infeasible toward the end of the operating time period. The proof of closed-loop stability and recursive feasibility of the LEMPC illustrated that for sufficiently small sampling period Δ and sufficiently small upper bound of the disturbance θ, the LEMPC is guaranteed to be feasible at each sampling time. Nevertheless, determining exactly the value of the upper bound of disturbance θ that can ensure feasibility of the LEMPC is difficult due to the nonlinearity and nonconvexity of the problem. In addition, incorporating the material constraint of Eq. (26) into both the classical LEMPC and the Safeness Index-based LEMPC does not allow guaranteeing *a priori* closed-loop stability and feasibility of both optimization problems. However, for the value of the upper bounds considered in this simulation $\left(\theta_1 = 1\ \frac{kmol}{m^3} \text{ and } \theta_2 = 20\,K\right)$, both optimization problems were feasible at each sampling time.

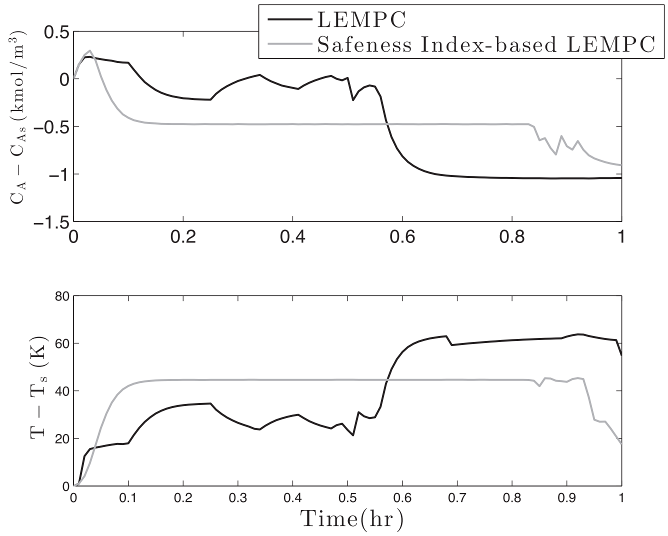

Fig. 9. The state profiles for the closed-loop CSTR under the LEMPC design of Eq. (12) and under the Safeness Index-based LEMPC design of Eq. (13) for the initial condition $x_{int}^T = \left[0\ \frac{kmol}{m^3}\quad 0\,K\right]$ with bounded process disturbances.

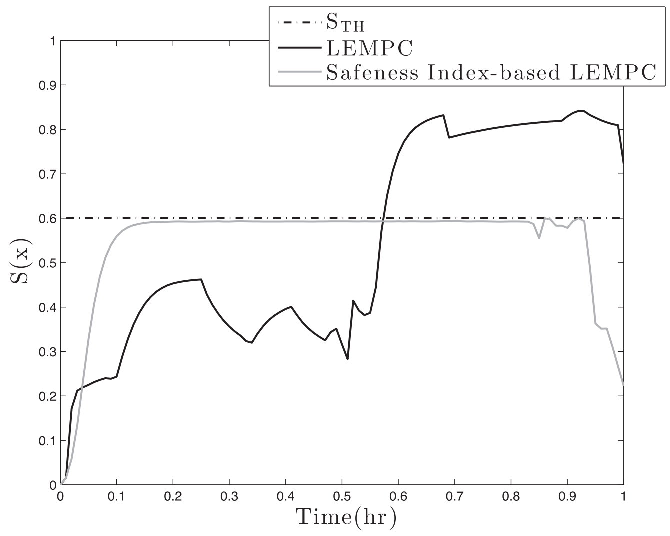

Fig. 10. The Safeness Index function $S(x)$ for the closed-loop CSTR under the LEMPC design of Eq. (12) and under the Safeness Index-based LEMPC design of Eq. (13) for the initial condition $x_{int}^T = \left[0\ \frac{kmol}{m^3}\quad 0\,K\right]$ with bounded process disturbances.

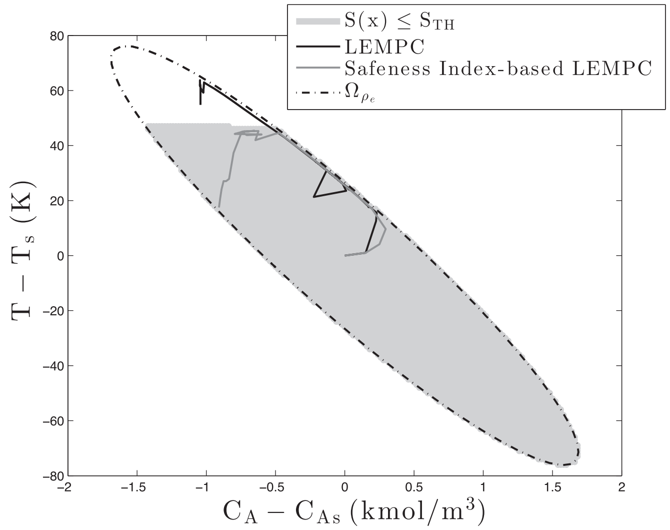

Fig. 11. The state-space profile for the closed-loop CSTR under the LEMPC design of Eq. (12) (black trajectory) and under the Safeness Index-based LEMPC design of Eq. (13) (dark gray trajectory) for the initial condition $x_{int}^T = \left[0\ \frac{kmol}{m^3}\quad 0\,K\right]$ with bounded process disturbances.

5. Conclusion

In this work, a Safeness Index was developed that can coordinate, for the first time, the control and safety systems within a chemical process plant. Specifically, an approach for defining the functional form of the Safeness Index $S(x)$ was presented, and a methodology of choosing the threshold S_{TH} of the Safeness Index $S(x)$ was given. To demonstrate the use of this Safeness Index within a control system, an LEMPC scheme with a hard Safeness Index-based constraint was presented to integrate feedback control, process safety and process economics within a unified framework. An implementation strategy was developed that is guaranteed, under sufficient conditions, to drive the closed-loop state into the region where the Safeness Index is less than a desired threshold when initiated from any state within the stability region. The proposed method was demonstrated through a chemical process example to be capable of maintaining the closed-loop state within a safe region of operation while maximizing process economics. An illustration of how to define the Safeness Index $S(x)$ and its threshold was given in the context of a non-isothermal continuous stirred tank reactor (CSTR) example where the temperature of the reactor has the largest effect on the safeness of the process.

Acknowledgements

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

References

Ahooyi, T.M., Soroush, M., Arbogast, J.E., Seider, W.D., Oktem, U.G., 2016. Model-predictive safety system for proactive detection of operation hazards. AIChE J. 62, 2024–2042.

AIChE, 1994a. Dow's Chemical Exposure Index Guide, First ed. AIChE, New York, NY.

AIChE, 1994b. Dow's Fire and Explosion Index Hazard Classification Guide, Seventh ed. AIChE, New York, NY.

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

Albalawi, F., Durand, H., Alanqar, A., Christofides, P.D., 2017. Achieving operational process safety via model predictive control. J. Loss Prev. Process Ind., in press.

Atherton, J., Gil, F., 2008. Incidents that Define Process Safety. John Wiley & Sons, Hoboken, NJ.

Christofides, P.D., El-Farra, N.H., 2005. Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-Delays. Springer-Verlag, Berlin, Germany.

Chylla, R.W., Adomaitis, R.A., Çinar, A., 1987. Stability of tubular and autothermal packed bed reactors using phase plane analysis. Ind. Eng. Chem. Res. 26, 1356–1362.

Crowl, D.A., Louvar, J.F., 2011. Chemical Process Safety: Fundamentals with Applications, Third ed. Pearson Education, Upper Saddle River, NJ.

El-Farra, N.H., Christofides, P.D., 2003. Bounded robust control of constrained multivariable nonlinear processes. Chem. Eng. Sci. 58, 3025–3047.

Heidarinejad, M., Liu, J., Christofides, P.D., 2012. Economic model predictive control of nonlinear process systems using Lyapunov techniques. AIChE J. 58, 855–870.

Khalil, H.K., 2002. Nonlinear Systems, Third ed. Prentice Hall, Upper Saddle River, NJ.

Khan, F.I., Abbasi, S.A., 1999. Major accidents in process industries and an analysis of causes and consequences. J. Loss Prev. Process Ind. 12, 361–378.

Kidam, K., Hurme, M., 2013. Analysis of equipment failures as contributors to chemical process accidents. Process Saf. Environ. Prot. 91, 61–78.

Kletz, T., 2009. What Went Wrong? – Case Histories of Process Plant Disasters and How They Could Have Been Avoided, Fifth ed. Elsevier, Burlington, MA.

Kokotović, P., Arcak, M., 2001. Constructive nonlinear control: a historical perspective. Automatica 37, 637–662.

Latham, D.A., McAuley, K.B., Peppley, B.A., Raybold, T.M., 2011. Mathematical modeling of an industrial steam-methane reformer for on-line deployment. Fuel Process. Technol. 92, 1574–1586.

Leveson, N.G., 1995. Safeware: System Safety and Computers. Addison-Wesley Publishing Company, Reading, MA.

Leveson, N.G., Stephanopoulos, G., 2014. A system-theoretic, control-inspired view and approach to process safety. AIChE J. 60, 2–14.

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

Muñoz de la Peña, D., Christofides, P.D., 2008. Lyapunov-based model predictive control of nonlinear systems subject to data losses. IEEE Trans. Autom. Control 53, 2076–2089.

Mannan, M.S., Sachdeva, S., Chen, H., Reyes-Valdes, O., Liu, Y., Laboureur, D.M., 2015. Trends and challenges in process safety. AIChE J. 61, 3558–3569.

Marlin, T., 2012. Operability in Process Design: Achieving Safe, Profitable, and Robust Process Operations. McMaster University, Ontario, Canada.

Massera, J.L., 1956. Contributions to stability theory. Ann. Math. 64, 182–206.

Mayne, D.Q., Rawlings, J.B., Rao, C.V., Scokaert, P.O.M., 2000. Constrained model predictive control: stability and optimality. Automatica 36, 789–814.

Mhaskar, P., Liu, J., Christofides, P.D., 2013. Fault-Tolerant Process Control: Methods and Applications. Springer-Verlag, London, England.

Pariyani, A., Seider, W.D., Oktem, U.G., Soroush, M., 2010. Incidents investigation and dynamic analysis of large alarm databases in chemical plants: A fluidized-catalytic-cracking unit case study. Ind. Eng. Chem. Res. 49, 8062–8079.

Rawlings, J.B., 2000. Tutorial overview of model predictive control. IEEE Control Syst. Mag. 20, 38–52.

Reniers, G., Cozzani, V. (Eds.), 2013. Domino Effects in the Process Industries: Modeling, Prevention and Managing. Elsevier, Waltham, MA.

Smith, H., Howard, C., Foord, T., 2003. Alarms management/Priority, floods, tears or gain? Introduction to the “problem”. Meas. Control 36, 109–113.

Tatiya, R.R., 2011. Elements of Industrial Hazards: Health, Safety, Environment and Loss Prevention. CRC Press/Balkema, Leiden, Netherlands.

Venkatasubramanian, V., 2011. Systemic failures: challenges and opportunities in risk management in complex systems. AIChE J. 57, 2–9.

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

Wang, J., Yang, F., Chen, T., Shah, S.L., 2016. An overview of industrial alarm systems: main causes for alarm overloading, research status, and open problems. IEEE Trans. Autom. Sci. Eng. 13, 1045–1061.