Computers and Chemical Engineering 114 (2018) 171–190

Contents lists available at ScienceDirect

Computers and Chemical Engineering

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

Process operational safety via model predictive control: Recent results and future research directions

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

[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 20 June 2017
Accepted 9 October 2017
Available online 6 November 2017

Keywords:
Process safety
Process control
Model predictive control
Process operation
Nonlinear processes
Safety systems

ABSTRACT

The concept of maintaining or enhancing chemical process safety encompasses a broad set of considerations which stem from management/company culture, operator procedures, and engineering designs, and are meant to prevent incidents at chemical plants. The features of a plant design that take action to prevent incidents on a moment-by-moment basis are the control system and the safety system (i.e., the alarm system, safety instrumented system, and safety relief system). Though the control and safety systems have a common goal in this regard, coordination between them has been minimal. One impediment to such an integrated control-safety system design is that the traditional industrial approach to safety focuses on root causes of incidents and on keeping individual measured variables within recommended ranges, rather than seeking to understand incidents from a more fundamental perspective as the result of the dynamic process state evolving to a value at which consequences to humans and the environment occur. This work reviews the state of the art in control system designs that incorporate explicit safety considerations in the sense that they have constraints designed to prevent the process state from taking values at which incidents can occur and in the sense that they are coordinated with the safety system. The intent of this tutorial is to unify recent developments in this area and to encourage further research by showcasing that the topic, though critical for safe operation of chemical processes particularly as we move to more tightly integrated and economics-focused operating strategies, is in its infancy and that many open questions remain.

1. Introduction

Due to the dangers to people and the environment that are inherent in operating chemical processes, process safety has been an important consideration for both the design and operation of chemical processes throughout time (Crowl and Louvar, 2011). The concept of ensuring process safety is very broad and is often considered to refer to appropriate engineering designs that prevent incidents in the presence of abnormal operating conditions, combined with management decisions, training, and procedures put in place at a site to protect people and the environment against hazards so that the risk of incidents can be mitigated (Center for Chemical Process Safety, 2010, 2001). The definition of "incidents" broadly includes all situations termed "near misses" or "accidents" of various severity levels in industry that are considered to have had the potential to lead to hazards to people, the environment, or property, or that did lead to harm (Jones et al., 1999; Phimister et al., 2003). The prevention of incidents at a plant is considered to involve both human engagement (at the level of procedure development and daily execution of these procedures, and also at the level of determining what unexpected scenarios may occur for which barriers to incidents should be set up through techniques such as Hazard and Operability (HAZOP) studies and fault tree analysis Center for Chemical Process Safety, 2008) and the success of automation at the plant (e.g., software functioning according to the expectations of those who install it Leveson (1995), the safety instrumented system functioning properly, and the control system regulating process variables to their steady-state values). The multifaceted nature of process safety as described above has caused it to be addressed from many different angles. Some of the topics that have been addressed in the literature include automating aspects of the engineering judgment process (Venkatasubramanian et al., 2000), preventing fires and explosions and understanding the effects of chemical release (Englund, 2007; Reniers and Cozzani, 2013), designing processes to be inherently safe

[*] Corresponding author at: Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA.
E-mail address: pdc@seas.ucla.edu (P.D. Christofides).

https://doi.org/10.1016/j.compchemeng.2017.10.006
0098-1354/© 2017 Elsevier Ltd. All rights reserved.

(Khan and Amyotte, 2003), studying past incidents (Kidam and Hurme, 2013; Kletz, 2009), quantifying the risk associated with incidents (Center for Chemical Process Safety, 2000), and dynamic failure assessment (Meel and Seider, 2006). An additional consideration is that incidents do not necessarily occur during continuous process operation, but may also occur under atypical operating conditions, such as when the plant is off-line during maintenance or is being started up (Ness, 2015; Bloch, 2016). In this work, we will focus on the aspect of process safety related to designing equipment that takes action in response to a certain stimulus (the control system and safety system, which in this work is defined to include the alarm (Rothenberg, 2009), safety instrumented (Mannan, 2012; Center for Chemical Process Safety, 2017b), and safety relief systems Center for Chemical Process Safety, 1998; Fisher et al., 1992) to prevent incidents at a plant. Therefore, the references to “process safety” and “process operational safety” throughout this work should be understood in this context.

The control system and the safety system complement one another as part of an approach to maintaining operational safety in the chemical process industries which can be considered, at a high level, to be hierarchical according to Fig. 1. The control system is typically used to regulate process states like temperature and pressure to their steady-state values in the presence of disturbances. The alarms will be triggered when process variable measurements either exceed certain thresholds (when the threshold represents an upper bound) or fall below them (when the threshold represents a lower bound) (Pariyani et al., 2010) due to, for example, disturbances or equipment faults, and the alarm system will supply some information to an operator regarding the reason for the alarm system activation so that the operator has a chance to take corrective actions based on the alarm. Other thresholds on measured process variables are set such that the safety instrumented system will take automated actions with an on/off characteristic (e.g., it may fully close a valve for the fuel stream to a reactor to shut off the process completely) when the process variables exceed/fall below these thresholds. The safety relief system is often comprised of valves or rupture disks that are mechanically actuated (e.g., they open or burst due to the properties of the materials from which they are made when a certain pressure builds up behind the valves/disks). Safety relief devices are typically used with vessels within which the pressure can rise and lead to explosion of the vessel if the pressure is not reduced by the valves/rupture disks. When necessary, containment of chemical releases or emergency response plans are utilized (Marlin, 2012). Standard practice emphasizes the independence of the control system and the elements of the safety system in the sense that failure of critical components of the control, alarm, safety instrumented, or relief system should not cause failure of the other systems. It is worth investigating, however, how the control and safety systems may be designed to account for limitations of one another (e.g., the control system could anticipate the activation of the safety system through state predictions during process operation and the safety system could be triggered by state-based considerations typically only accounted for in the control design) without sacrificing redundancy in the design. Coordination between the control and safety systems has traditionally been limited; it may involve, for example, determining how close the controller needs to keep the process state to an operating steady-state (and what that means for the controller’s design) to avoid activating elements of the safety system as much as possible (Center for Chemical Process Safety, 2017a), or it may involve state constraints on predicted states in control designs that explicitly handle constraints (Qin and Badgwell, 2003).

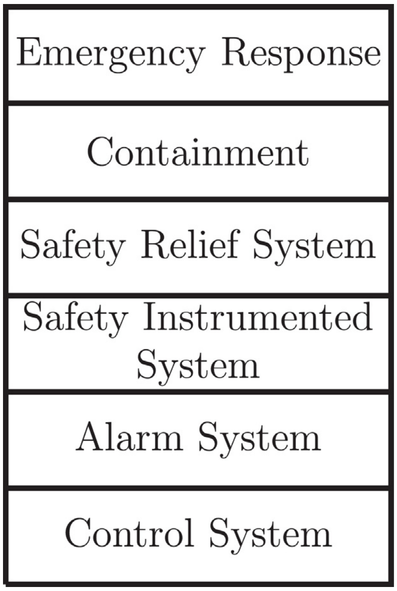

Fig. 1. Hierarchical approach to maintaining operational safety (Marlin, 2012).

Greater coordination of the control and safety systems may be beneficial given the complementary roles of those systems in preventing incidents and also the typical hierarchical nature of their use (i.e., if the control system does not prevent a measured process state from crossing a threshold, an alarm sounds; this indicates that the way that the control system functions directly impacts whether the safety system needs to take action). A starting point for pursuing this greater coordination is designing the control system to explicitly account for safety considerations so that under normal process operation, the process state is maintained in a region in state-space where incidents are not expected to occur and where the safety system is not activated. The concept of incorporating safety within control (specifically, within model predictive control (MPC) (Qin and Badgwell, 2003; Ellis et al., 2016), which will be the focus of this paper due to the industrial relevance of MPC and its ability to account for constraints and multivariable interactions that can be important for analyzing whether the process state is within regions in state-space where incidents may occur) has been associated primarily with closed-loop stability and robustness arguments, incorporation of safety metrics in control design, and designing controllers to respond to changes in the process dynamics or available equipment over time. In this tutorial, we highlight the need for characterizing safe operating regions in state-space using safety metrics that mathematically formalize the concept of a systems approach to process operational safety (this systems perspective will be shown to result in safety-based constraints for MPC that are different from the types of state constraints traditionally considered to be related to operational safety), especially as there are greater pushes toward more integrated manufacturing paradigms that may operate processes in a time-varying fashion as opposed to the traditional steady-state fashion. We will also enumerate desirable properties for controllers that seek to maintain process safety, identifying fundamental benefits and limitations of different control designs for achieving these desirable properties. We will conclude with an outlook on how a system-theoretic safety metric may impact safety system design and an outlook on further advances that will enable greater coordination between the control and safety systems to prevent incidents at chemical plants.

2. Preliminaries

2.1. Notation

The notation $|\cdot|$ signifies the Euclidean norm of a vector. The symbol $S(\Delta)$ signifies the class of piecewise-constant functions with period Δ. A function $\alpha : [0, a) \rightarrow [0, \infty)$ is said to be in class $\mathcal{K}$ if it is continuous, strictly increasing, and $\alpha(0) = 0$. A scalar-valued, continuous function $V(x) : R^n \to R$ is said to be positive definite if $V(x) > 0$ for all $x \in R^n$ except $x = 0$, and $V(0) = 0$. The notation Ω_ρ denotes a level set of a positive definite function $V(\cdot)$ (i.e., $\Omega_\rho := \{x \in R^n : V(x) \le \rho\}$). The notation $x \in A_1/B_1$, where A_1 and B_1 are sets, denotes the set of $x \in A_1$ such that $x \notin B_1$.

2.2. Class of nonlinear process systems

Unless otherwise noted, this tutorial will consider continuous time nonlinear process systems with the following state-space description:

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

where $x \in R^n$ is the process state vector, and $u \in R^m$ and $w \in R^l$ are the control (manipulated) input vector and the disturbance vector, respectively. The process state is assumed to be bounded within a set $X \subseteq R^n$. The admissible input values (the components u_i, $i = 1, \ldots, m$, of u) are restricted to be in m nonempty convex sets $U_i \subset R$, $i = 1, \ldots, m$, due to physical limitations on the actuation energy. We assume that w is bounded within the set $W := \{w \in R^l : |w| \le \theta, \theta > 0\}$. We assume that f is a locally Lipschitz vector function of its arguments and, without loss of generality, we assume that the origin of the system is an equilibrium (i.e., $f(0, 0, 0) = 0$; when there are multiple equilibria, we assume with slight abuse of notation that the vector function f has been translated to have its equilibrium at the steady-state of interest such that for the equilibrium under consideration, we can denote the right-hand side of Eq. (1) at the equilibrium by $f(0, 0, 0) = 0$). The dynamics of typical industrial chemical process systems fall within the class of systems of Eq. (1). Input-affine systems that fall within the class of systems of Eq. (1) are denoted by:

$$\dot{x} = \bar{f}(x) + \sum_{i=1}^{\bar{m}} g_i(x)\bar{u}_i + b(x)w \tag{2}$$

where $x \in X \subseteq R^n$, $w \in W \subset R^l$, and $\bar{f}$, g_i, $i = 1, \ldots, \bar{m}$, and b are locally Lipschitz vector functions that are assumed to be zero at an equilibrium (i.e., $\bar{f}(0) = 0$, $g_i(0) = 0$, $i = 1, \ldots, \bar{m}$, and $b(0) = 0$, where again with slight abuse of notation, $\bar{f}$, g_i, $i = 1, \ldots, \bar{m}$, and b denote translations of these vector functions to have their zero values at the equilibrium under consideration when there are multiple equilibria for the system of Eq. (2)). The vector $\bar{u}_i \in R^{m_i}$, $i = 1, \ldots, \bar{m}$, contains m_i, $i = 1, \ldots, \bar{m}$, components of the vector $u \in R^m$. Because $u_i \in U_i$, $i = 1, \ldots, m$, $\bar{u}_j \in \bar{U}_j$, $j = 1, \ldots, \bar{m}$, where $\bar{U}_j$ is the set defining the bounds on each u_i contained within $\bar{u}_j$. Throughout this review, we consider synchronous state measurements at sampling times denoted by $t_k = t_0 + k\Delta$, $k = 0, 1, \ldots$, where t_0 denotes the initial time and Δ denotes the sampling period. We also define the nominal process state trajectory as the trajectory of the nonlinear process system of Eq. (1) or (2) with $w(t) \equiv 0$.

3. Enforcing operational safety through control design

Three properties of control designs either explicitly or implicitly associated with maintaining operational safety in the literature are guaranteed closed-loop stability/robustness under normal operating conditions, guaranteed safety metric constraints satisfaction by computed control actions, and guaranteed closed-loop stability as process operating conditions change due to, for example, equipment faults. However, for controllers with these properties to be considered to maintain process safety, certain assumptions must be met on how operational safety can be represented for a given process. In this section, we elucidate these assumptions within a system-theoretic framework for process safety that characterizes operational safety as a property of the states, inputs, and disturbances of a system, and how they interact to cause the state to evolve in state-space in directions that affect the containment or release of chemicals. Based on the underlying safety-related assumptions for the various control formulations analyzed, we develop a list of desirable properties for a controller designed to ensure process operational safety to direct further research in this area.

All of the control designs to be discussed in the context described in the above paragraph will be MPC's. This is because the classical proportional-integral-derivative (PID) type controllers widely used in the process industries cannot take multi-variable interactions, unmeasured states, or actuator constraints explicitly into account, though these may be important for analyzing process safety, especially for nonlinear processes. Furthermore, they do not have the ability to incorporate knowledge of safety system triggers since they are not model-based controllers (in the sense of utilizing a process model explicitly in the calculation of control actions). However, MPC solves a constrained optimization problem subject to a process model to account for multi-variable interactions and closed-loop process dynamics and therefore can take proactive actions to prevent the process variables from taking values corresponding to abnormal process conditions, potentially decreasing the frequency with which elements of the safety system are triggered. It can also account for equipment faults (e.g., sensor and actuator faults) which PID-type control loops are not most suitable for handling. Therefore, MPC is an appropriate control design for analyzing the integration of process operational safety and control.

3.1. A systems approach to process operational safety

Several recent research works have proposed that concepts from systems engineering and control can be utilized to understand the causes of incidents at chemical plants and to prevent them (Mannan et al., 2015; Venkatasubramanian, 2011) (in general, however, the notion that a systems perspective can be valuable for preventing accidents for engineering systems is not limited to chemical processes; see, e.g., Kim and Kumar, 2014). For example, Bakolas and Saleh (2010) propose that the concept of observability from control theory can be used to analyze the circumstances under which hazardous operating conditions can be identified. Cowlagi and Saleh (2015) exemplify the use of coordinability and consistency principles for hierarchical multilevel systems for analyzing process incidents. Leveson and Stephanopoulos (2014) propose that the prevention of accidents at a plant must come from controlling and constraining the sociotechnical system that influences the design, maintenance, and operation of plants, and indicates that MPC provides an appropriate framework for understanding this. Though a number of these works that describe incident analysis and prevention as a systems problem view it in a broader context than we consider in this paper by restricting our focus to incident prevention using the control and safety systems, the principles in these other works have inspired the development of a systems approach to operational safety. Specifically, based on the concepts in works such as those described above that interactions between components at a chemical plant can induce hazardous conditions and that incidents are the result of a gradual evolution of the plant conditions to a condition at which the incident cannot be prevented, (Albalawi et al., 2017d) develops a mathematical characterization of operational safety by interpreting those concepts to mean that the process dynamic model is nonlinear with coupled states, such that the safeness of a process operating condition should depend on the process state. Albalawi et al. (2017d) therefore develops guidelines for creating a safety metric for a process termed the Safeness Index (denoted by $S(x)$) that is solely a function of the state (in the sense that it is not a function of the inputs or disturbances). It provides the following benefits as an indicator for process operational safety: (1) It is state-based: the Safeness Index can account for multivariable interactions that impact the possibility of incidents occurring at certain states, it can account for states exceeding allowable values, and it can also take advantage of state estimation techniques (e.g., Khalil and Esfandiari, 1993; Kazantzis and Kravaris, 1998) to account for unmeasured states that may be important to understanding the potential of an incident occurring; furthermore, it does not require that any information be known regarding how the state came to be at a given state, but only the current state measurement, to indicate the safeness of the process state; and (2) it is general: the Safeness Index can define regions of various shapes within which the Safeness Index is below a certain bound by setting thresholds on the index. The appropriate functional form of $S(x)$ is process-dependent, but it can be developed by following guidelines detailed in Albalawi et al. (2017d), which include analyses of first-principles process models, industrial safety studies, and process operating data. After developing the functional form of $S(x)$, a threshold S_{TH} can be set on $S(x)$ that distinguishes a desirable operating region (i.e., the region where $S(x) \leq S_{TH}$, which will be referred to as the safety zone in the remainder of this work) from an undesirable operating region (i.e., the region where $S(x) > S_{TH}$) for use in setting safety-based constraints within MPC design. The safety zone should be within a safe operating region (which throughout this article refers to a region in state-space where, if the process state were to remain there continuously, no incidents would be anticipated and the safety system would not be triggered), but does not necessarily have to include all of it (this is because the purpose of defining S_{TH} is to use it within the control design, so it does not have to be set to the maximum value that $S(x)$ takes within the safe operating region; therefore, there may be regions outside the safety zone that are still within a safe operating region). The value of S_{TH} will depend on the properties of the control design that it is used with and also process-specific considerations, but in all cases the threshold should be set to avoid incidents and safety system activation during normal process operation. To obtain an appropriate threshold, engineers can utilize first-principles models, traditional safety analysis tools, and past operating data as described in Albalawi et al. (2017d).

Another consideration for the development of $S(x)$ and S_{TH} is that they are developed to indicate the relative safeness of operating at a certain state of a dynamic system for which the dynamics may change over time due to, for example, heat exchanger fouling or catalyst deactivation, or disturbances such as a change in the composition of the feedstock that are persistent in the sense that they do not go away. As the process dynamics change, the functional form of the Safeness Index or the thresholds upon it may need to be updated to reflect the new operating conditions. Furthermore, the development of the process Safeness Index in Albalawi et al. (2017d) assumes that the Safeness Index is developed for a system without equipment faults; as faults become expected due to, for example, aging of the equipment or indications that equipment is not working properly based on process data, the Safeness Index and its threshold may need to be updated to reflect that certain states that can be considered safe to operate at (in the sense that incidents would not be expected to occur if the process operated continuously at that state) under non-faulty operating conditions would not be considered to be safe to operate at if an equipment fault occurred. Therefore, the Safeness Index and its thresholds may need to be updated on-line by engineers or potentially automated methods based on the value of the Safeness Index for immediate past operating data. No indication of how to adjust $S(x)$ or S_{TH} on-line as faults or disturbances occur is given in Albalawi et al. (2017d), but it is reasonable to assume that the methods proposed in Albalawi et al. (2017d) for the development of the original functional form of $S(x)$ and S_{TH} can be taken advantage of, particularly the suggestions of the use of process operating data which would likely contain important information on the changes in the process operating conditions necessitating the change in the Safeness Index form and threshold.

3.2. MPC designs that maintain closed-loop stability/robustness

An underlying assumption of much of the MPC literature is that the primary condition guaranteeing safety (i.e., that no incidents will occur during routine process operation) of a nonlinear process under the MPC design is closed-loop stability and/or robustness of the nonlinear process under the controller. Some works have explicitly made this connection (e.g., Aswani et al., 2013 refers to the combination of robustness and closed-loop stability as safety), whereas other works imply it through rigorous closed-loop stability analyses of a control design, at times even in the presence of disturbances (e.g., Morari and Lee, 1999; Mayne et al., 2000; Camacho and Bordons, 2007; Huang et al., 2012; Angeli et al., 2012). Closed-loop stability is typically understood in the MPC literature in one of two senses: (1) the process state is driven to an operating steady-state (assumed to be a safe point at which to operate given the impracticality of the alternative assumption) by the controller or (2) the process state is maintained within a bounded region of state-space by the controller (the concept of maintaining the system state within a desired set or keeping it out of undesired sets has been associated with prevention of problematic behavior for various engineering systems, e.g., Wieber, 2008; Carson et al., 2013; Gillula et al., 2010; Abate et al., 2008). If closed-loop stability could not be expected in either sense for a process operated under MPC, there is a possibility that states that play a key role in preventing chemical release or explosion like temperature and pressure could approach dangerous values because there is no guarantee that they are maintained within expected ranges by a control system (not knowing where the states will lie in state-space during normal process operation may also increase activations of the safety system as it tries to prevent incidents that are not being prevented by the control system due to inadequate control system design). However, while closed-loop stability is a critical component of maintaining process safety, we will clarify in this section that the region in state-space from which the closed-loop state can be mathematically guaranteed to be driven to the steady-state or maintained in a region around it is not necessarily the same as a safe operating region, and that therefore those works which associate closed-loop stability, either implicitly or explicitly, with safety considerations make underlying assumptions on the characterization of a safe operating region in state-space (and, because the Safeness Index discussed in the prior section for characterizing process safety is a state-based metric, such underlying assumptions can be cast in terms of assumptions on the Safeness Index form and thresholds).

To discuss closed-loop stability of a nonlinear process under MPC, we present a general form of an MPC with state constraints, which is formulated as an optimization problem that is solved to determine the values of the manipulated inputs to apply to the process:

$$\max_{u(t) \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau)) \; d\tau \tag{3a}$$

$$\text{s.t.} \;\; \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{3b}$$

$$u_i(t) \in U_i, \quad i = 1, \ldots, m, \; \forall t \in [t_k, t_{k+N}) \tag{3c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{3d}$$

$$\tilde{x} \in X, \; \forall \;\; t \in [t_k, t_{k+N}) \tag{3e}$$

where $L_e(\tilde{x}(\tau), u(\tau)) : R^n \times R^m \rightarrow R$ in Eq. (3a) is a general stage cost (i.e., no specific functional form of the stage cost is required) that is optimized over a prediction horizon of N sampling periods of length Δ by choosing input trajectories $u \in S(\Delta)$ (i.e., N piecewise-constant manipulated input trajectories are computed, one for each sampling period of the prediction horizon). Eq. (3b) is a constraint requiring that all predictions $\tilde{x}$ of the process state in the objective function and the state constraint of Eq. (3e) must come from solving the model of the nominal system of Eq. (1) subject to the initial condition (obtained from a state measurement at time t_k) of Eq. (3d). Eq. (3c) represents the constraint on the manipulated inputs. In general, additional constraints on the state besides those in Eq. (3e) can be added to the optimization problem as well. Because the MPC objective function is not restricted to the tracking form (a tracking stage cost would take a form $L_e = x^T Q_T x + u^T R_T u$, where Q_T and R_T are positive definite matrices) which is common in industrial implementations of MPC in the chemical process industries, the MPC design of Eq. (3) falls within the category of economic model predictive control (Ellis et al., 2014a; Rawlings et al., 2012; Müller and Allgöwer, 2017), which is an MPC design with a general objective function.

Depending on the prediction horizon length, process model/objective function form, and additional constraints of the optimization problem, different guarantees on closed-loop stability can be made for MPC with a general objective function. For example, some MPC formulations (e.g., those that add a terminal constraint to Eq. (3) requiring the state to equal the steady-state (Diehl et al., 2011) or be in a neighborhood of it Amrit et al. (2011), Alessandretti et al. (2016) at the end of the prediction horizon) allow closed-loop stability to be proven in the absence of disturbances (under several assumptions including initial feasibility of the optimization problem) in the sense that the closed-loop state is maintained within the feasible set at all times. Though this feasible set cannot be mathematically characterized *a priori* without closed-loop simulations due to the dependence of the terminal constraint on the prediction horizon length, the state constraints of Eq. (3e) are guaranteed to be satisfied within the feasible set, so if these state constraints are cast in a form related to the Safeness Index (because the Safeness Index is a state-based metric, any constraints on it would appear as state constraints), the MPC would maintain the state within a region where system-theoretic safety constraints are met. However, in the presence of disturbances, there is no guarantee that the state can be maintained within or driven back into the feasible set, though that set may correspond to a safe operating region; this indicates that the following property of MPC's designed to integrate control and safety is desirable.

Desirable Property 1. The MPC design should have guaranteed closed-loop stability properties in the presence of disturbances.

We now demonstrate that closed-loop stability of a nonlinear process under an MPC design and robustness of the controller are insufficient for ensuring that the process state is maintained in a safe operating region by the MPC unless the states from which the stability and robustness properties are mathematically guaranteed have been determined to be in a safe operating region using system-theoretic considerations. To develop this discussion, we make the following assumption (Khalil, 2002).

Assumption 1. There exists an explicit stabilizing controller $h(x) = [h_1(x) \cdots h_m(x)]^T$ that can asymptotically stabilize the origin of the nominal closed-loop system of Eq. (1) in the sense that there exists a sufficiently smooth positive definite Lyapunov function $V(x)$ and class $\mathcal{K}$ functions α_1, α_2, α_3, and α_4 such that the following inequalities hold for all x contained within a neighborhood $D \subseteq R^n$ of the origin:

$$\alpha_1(|x|) \le V(x) \le \alpha_2(|x|) \tag{4a}$$

$$\frac{\partial V(x)}{\partial x} f(x, h(x), 0) \le -\alpha_3(|x|) \tag{4b}$$

$$\left| \frac{\partial V(x)}{\partial x} \right| \le \alpha_4(|x|) \tag{4c}$$

$$h_i(x) \in U_i, \ i = 1, \ldots, m \tag{4d}$$

We define the stability region of the process of Eq. (1) under the Lyapunov-based controller $h(x)$ to be a level set of $V(x)$ within D where the state constraints are met (i.e., $x \in X$), and we denote the stability region by $\Omega_\rho := \{x \in D : V(x) \le \rho\}$, where $\Omega_\rho \subseteq X$. Techniques for developing explicit stabilizing controllers can be found in works such as Christofides and El-Farra (2005), Kokotović and Arcak (2001), Lin and Sontag (1991).

Using this notation, we now define two additional constraints that can be added to the MPC design of Eq. (3) to form Lyapunov-based MPC or LMPC (Heidarinejad et al., 2012; Mhaskar et al., 2006), which is a control design that is able to guarantee that the closed-loop state is maintained within an *a priori* explicitly characterizable, bounded region in state-space at all times even in the presence of disturbances. The two constraints are as follows:

$$V(\tilde{x}(t)) \le \rho_e, \ \forall t \in [t_k, t_{k+N}), \quad \text{if} \ \ x(t_k) \in \Omega_{\rho_e} \tag{5a}$$

$$\begin{aligned} &\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \le \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0), \\ &\text{if} \ \ x(t_k) \in \Omega_\rho / \Omega_{\rho_e} \ \ \text{or} \ \ t_k > t_s \end{aligned} \tag{5b}$$

where the notation follows that in Eq. (3) and t_s is a pre-set time after which it is desired to apply the constraint of Eq. (5b) for all subsequent times. The Lyapunov function value along the predicted state trajectory $\tilde{x}(t)$ is maintained within Ω_{ρ_e} by the constraint of Eq. (5a) when the state measurement at t_k is within Ω_{ρ_e}. The region Ω_{ρ_e} is chosen with ρ_e sufficiently small such that if the measured state $x(t_k)$ is within Ω_{ρ_e}, then $x(t_{k+1})$ is still within Ω_ρ even in the presence of uncertainty (an appropriate value of ρ_e may be obtained, for example, through extensive closed-loop simulations of a nonlinear process under the LMPC of Eq. (3) with the added constraints of Eqs. (5a) and (5b)). The constraint of Eq. (5a) allows the MPC to compute an input policy that permits the predicted closed-loop state to evolve in a time-varying fashion throughout Ω_{ρ_e} when the constraint of Eq. (5b) is not activated. When the contractive constraint of Eq. (5b) is activated (i.e., $x(t_k) \in \Omega_\rho / \Omega_{\rho_e}$ or $t_k > t_s$), the control actions computed by the LMPC will decrease the Lyapunov function value along the nominal closed-loop state trajectory by at least as much as the Lyapunov-based controller would at t_k (when implemented in sample-and-hold, a Lyapunov-based controller that meets Eq. (4) is guaranteed to decrease the Lyapunov function value throughout a sampling period for any initial state in Ω_ρ outside of a neighborhood of the origin Ω_{ρ_s} as long as Δ, ρ_e, and θ are sufficiently small Mũnoz de la Peña and Christofides, 2008).

The MPC of Eq. (3) with the added constraints of Eqs. (5a) and (5b) can maintain the process state in Ω_ρ at all times, even in the presence of sufficiently small disturbances; however, if the state constraints are not defined with respect to system-theoretic safety considerations, then even if $\Omega_\rho \subseteq X$, there is no guarantee that all of Ω_ρ will correspond to a safe operating region. This is because the stability region is defined mathematically following Assumption 1, but the mathematics are not necessarily tied to physical considerations. For example, for a process model defined by the two states of temperature and concentration, the state-space region from which it can be mathematically proven that a control law $h(x)$ could drive the process state to the steady-state may include states that are at a higher temperature than that at which the reactor material can safely be maintained without decreasing the service life (for example, the lifetime of reforming tubes in a steam methane reformer can be significantly decreased as the tube temperature is increased Pantoleontos et al., 2012). The reason that this disconnect between the stability region and the safe operating region in this case occurs is because the process model for which the stability region is characterized does not include how the reactor material behaves. This example indicates that properties of a system that are important to understanding the potential for incidents are often excluded from the model of a process being controlled so therefore an independent evaluation of the relative safeness of operating at each point in state-space should be undertaken. This leads to the second desirable property of an MPC designed to maintain process operational safety.

Desirable Property 2. The MPC should have constraints designed to maintain the process state in a safe operating region (defined by analyzing operational safety in a system-theoretic context).

This property is important for tracking MPC because it may help to prevent the state from moving out of a safe operating region on its way to the steady-state. It is also critical to account for system-theoretic safety considerations in control designs as we move toward more integrated and economics-focused operating strategies like the time-varying operating policy that may be set up under MPC with a general objective function. Such MPC's may move the process state throughout the stability region purposely and even cause the state to remain at the boundary of the stability region or in certain regions of the stability region not local to the steady-state to optimize the objective function; without system-theoretic metrics constraining the state as it is driven throughout the stability region by the MPC, the state may move out of a safe operating region.

Two other key considerations in the MPC literature in addition to stability and robustness have been feasibility and economic performance of a nonlinear process under the control design. Though in general these properties are not critical to maintaining operational safety (as we shall discuss in later sections, infeasibility of an MPC optimization problem can be dealt with by applying alternative control designs (i.e., control designs with characterizable properties in the sense that any constraints met by the alternative control inputs are known) when the MPC becomes infeasible, and maintaining operational safety is always a more important operating objective than maximizing process economic performance), they are indicative of the following two additional desirable properties for MPC designs that aim to maintain process operational safety.

Desirable Property 3. Safety-based constraints should be designed using good engineering judgment to set safety as the highest priority without unnecessarily sacrificing economic performance.

Desirable Property 4. Only characterizable inputs should be applied to a process.

The above analysis indicates that works on MPC designs with closed-loop stability guarantees that do not explicitly define a functional relationship between safety and the state constraints implicitly assume that the set of initial states for which closed-loop stability of a nonlinear process under the controller is guaranteed are within the region that would be designated as a safe operating region if a system-theoretic analysis of the safeness of each of the states in that set was performed.

3.3. MPC designs with safety-based state constraints

The next category of MPC's that have been associated with maintaining operational safety are designs with constraints on process states. A number of papers (e.g., de Oliveira Kothare and Morari, 2000) note that state constraints in MPC are often considered to be safety-related, and Piché et al. (2000) clarifies the common notion of safety-related state constraints by stating that an upper bound on temperature in an exothermic reactor is an example of such a constraint; pressure is also indicated in Mayne et al. (2000) to be a safety-related state that may be constrained. These bounds on individual states, however, are more in line with the traditional industrial safety thinking where each variable is examined individually than with the system-theoretic thinking described in Section 3.1 in which nonlinear interactions between variables also play a role in process operational safety. This reveals that an underlying assumption of the literature with traditional state constraints on process variables for safety purposes is that the states that are constrained in a traditional MPC (e.g., temperature or pressure) are the only states that would appear in a system-theoretic safety metric like the Safeness Index developed for the process and that they would appear in the uncoupled fashion that they appear in traditional state constraints (e.g., $S(x) \leq S_{TH}$ would not represent that a combination of temperature and pressure are required to be maintained less than a threshold, but would instead represent that temperature and pressure be less than individual thresholds). When closed-loop stability or robustness properties are not analyzed for an MPC with state constraints implemented for safety reasons (e.g., Wu et al., 2017, where an upper bound on the temperature in a reforming tube is used to prevent incidents due to decreases in the reforming tube life), another underlying assumption of the control design is that it can maintain closed-loop stability even in the presence of disturbances (because this was described in the prior section to be important for a control design ensuring operational safety).

A recently developed control design imposes state constraints on the Safeness Index and also rigorously analyzes its closed-loop stability and robustness properties (Albalawi et al., 2017d) and thus serves as the first mathematical formalization of incorporating system-theoretic safety considerations within MPC according to the vision of Section 3.1. Because this is the first design that builds toward the vision of an integrated control-safety system that we seek to lay out in this paper, we will spend several subsections to review its properties.

3.3.1. Safeness Index-Based MPC: formulation comparison with stability region-based safety concepts

The general form of a model predictive control design with a Safeness Index-based constraint to explicitly account for operational safety considerations in a systems context is as follows:

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

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

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

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

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

$$\begin{aligned} & S(\tilde{x}(t)) \leq S_{TH}, \quad \forall t \in [t_k, t_{k+N}) \\ & \text{if} \;\; S(x(t_k)) \leq S_{TH} \end{aligned} \tag{6f}$$

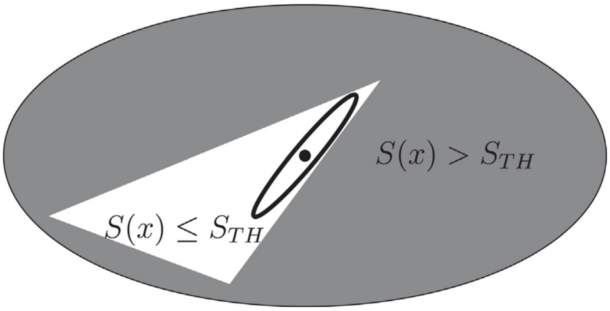

Fig. 2. Example of a region in state-space partitioned based on $S(x)$ (the gray region signifies the region where $S(x) > S_{TH}$ and the white region signifies the region where $S(x) \leq S_{TH}$) in which a level set of $V(x)$ within the safety zone (represented by the dark-outlined ellipse within the region where $S(x) \leq S_{TH}$ and containing the circle that represents the origin) may be much smaller than the region where $S(x) \leq S_{TH}$.

$$\begin{aligned}&\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0)\\ &\leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0),\\ &\text{if } \ x(t_k) \in \Omega_\rho/\Omega_{\rho_e} \ \text{ or } \ t_k > t_s \ \text{ or } \ S(x(t_k)) > S_{TH}\end{aligned} \tag{6g}$$

where the notation follows that in Eqs. (3) and (5). As noted in Albalawi et al. (2017d), other constraints on the Safeness Index instead of the hard bound of Eq. (6f) (e.g., a constraint on the integral of $S(x)$ over time or a constraint on the time that $S(x)$ spends above a threshold) may be considered as well, though without guarantees of feasibility (which is an issue for the constraint of Eq. (6f) as well as will be discussed below). The constraints of Eqs. (6e) and (6g) function similarly to the constraints of Eqs. (5a–5b) (i.e., they maintain the state within $\Omega_\rho \subseteq X$ over time such that it is not necessary to require explicitly in Eq. (6) that the constraint of Eq. (3e) be met; in this design, X refers to the state constraints besides those incorporating the Safeness Index). The constraint of Eq. (6f) requires that the predicted closed-loop state remain within the safety zone throughout the prediction horizon when the measurement of the state at t_k is within the safety zone. Because the stage cost L_e is general, this MPC design can be formulated as a tracking MPC by developing a quadratic stage cost with its minimum at a process steady-state and setting $t_s = t_0$ so that the contractive constraint of Eq. (6g) is enforced for all times.

The design of Eq. (6) is a version of the LMPC in Eqs. (3) and (5) augmented with Safeness Index-based constraints. However, it is not in general equivalent to that LMPC even if $\tilde{x} \in X$ were to signify that a Safeness Index-based constraint must be met by the control actions and Ω_ρ is contained within the set where the state constraints are met (i.e., $\Omega_\rho \subseteq X$). To see that the MPC of Eq. (6) is different than this, we can examine Fig. 2, which shows a dark gray stability region (for which it is assumed that a controller meeting Assumption 1 can drive the state from any initial condition in that stability region to the origin) within which is a triangularly shaped white region where $S(x) \leq S_{TH}$. Within the region where $S(x) \leq S_{TH}$ is a dark-outlined ellipse assumed to be representative of a Lyapunov level set with upper bound $\hat{\rho}$ contained within the region where $S(x) \leq S_{TH}$ (i.e., $\Omega_{\hat{\rho}}$ is contained in the region in Fig. 2 where the state constraints are met). The MPC of Eq. (5) would seek to maintain the state predictions within $\Omega_{\hat{\rho}}$. The MPC of Eq. (6), however, seeks to maintain the state predictions within the full white region and defines Ω_ρ in Eqs. (6e) and (6g) as the full ellipse in the figure (i.e., both the gray and white portions). This means that the process state predictions are allowed to evolve within a potentially larger region than they would be able to if the state predictions were forced to stay within $\Omega_{\hat{\rho}}$. This may allow greater economic benefits to be obtained while the state predictions are kept within a safe operating region (Desirable Property 3).

3.3.2. Safeness Index-Based MPC: fundamental benefits and limitations of general Safeness Index-based constraints

The greater freedom of the design of Eq. (6) compared to that which would be obtained if the state was forced to stay within a Lyapunov level set within the region where $S(x) \leq S_{TH}$ does come with a cost; specifically, the process state is not guaranteed to stay within the safety zone (i.e., the safety zone is not a forward invariant set for a process operated under the MPC of Eq. (6)). The reasons for this will be elucidated through some discussion of the closed-loop stability properties of the MPC of Eq. (6), for which the discussion relies on an assumption based on the following definition.

Definition 1. Let Assumption 1 hold and V be a Lyapunov function that satisfies Eq. (4) for the nominal process of Eq. (1) under $h(x)$ and Ω_ρ be the stability region. Define $\rho_{\min} < \rho$ by

$$\rho_{\min} = \max\{V(\bar{x}(t + \Delta)) : V(\bar{x}(t)) \leq \rho_s\} \tag{7}$$

where $0 < \rho_s < \rho_{\min}$ and $\bar{x}(t)$ signifies the solution of Eq. (1) under a sequence of sample-and-hold control actions with $u_i \in U_i$, $i = 1, \ldots, m$.

This definition of $\rho_{\min}$ allows it to be defined as a level set based on the maximum value of $V(x)$ reached in a sampling period even in the presence of bounded disturbances under any control action within the input constraints held throughout the sampling period when the value of $V(x)$ at the beginning of the sampling period is within a level set $\Omega_{\rho_s} \subset \Omega_{\rho_{\min}}$. The magnitude of $\rho_{\min}$ thus depends on Δ, θ, ρ_s, and U_i, $i = 1, \ldots, m$; not all conceivable values of those properties will allow a $\rho_{\min} < \rho$ to be defined. However, assuming that $\rho_{\min}$ can be found for a given Δ, θ, ρ_s, and U_i, $i = 1, \ldots, m$, combination, no sample-and-hold control action within the input bounds can drive $x(t)$ out of $\Omega_{\rho_{\min}}$ within Δ if $x(t_k) \in \Omega_{\rho_s}$, regardless of the type of controller used to compute the control action (e.g., Safeness Index-based MPC or $h(x)$ in sample-and-hold).

With the definition of $\Omega_{\rho_{\min}}$, we can now state the assumption that allows the closed-loop stability results to be described for the Safeness Index-based MPC.

Assumption 2. The Lyapunov level set $\Omega_{\rho_{\min}}$ from Definition 1 is contained within the region where $S(x) \leq S_{TH}$.

Notably, since $\Omega_{\rho_{\min}}$ contains the origin, the safety zone contains the origin as well. With Assumptions (1) and (2), a sufficiently small sampling period Δ, a sufficiently small bound θ on the norm of the disturbance vector, and a sufficiently small ρ_e value, the Safeness Index-based MPC design of Eq. (6) guarantees that when the Safeness Index-based MPC is feasible at every sampling time, (a) the closed-loop state is always bounded in Ω_ρ, (b) the closed-loop state is always driven into the safety zone in finite time when it is initialized outside of the safety zone, and (c) when $t_k > t_s$, the closed-loop state is ultimately bounded within $\Omega_{\rho_{\min}}$ (these properties labeled (a)–(c), which hold even in the presence of disturbances, will be referred to as stability properties (a)–(c) in the remainder of this tutorial for ease of discussion).

Feasibility of the Safeness Index-based MPC design is not guaranteed, however, because the region where $S(x) \leq S_{TH}$ (the safety zone) in which it is desired that the process state remain in general (in the sense that the constraint of Eq. (6f) is enforced on the predicted state and the contractive constraint of Eq. (6g) is designed to guarantee that the closed-loop state can be driven back into the safety zone in finite time) may have an irregular shape that is defined by safety considerations but is not defined with respect to a control design that can maintain the process state always within the safety zone (i.e., it is not defined like Ω_ρ, which is defined with respect to $h(x)$). In particular, the shape may not be related to $h(x)$

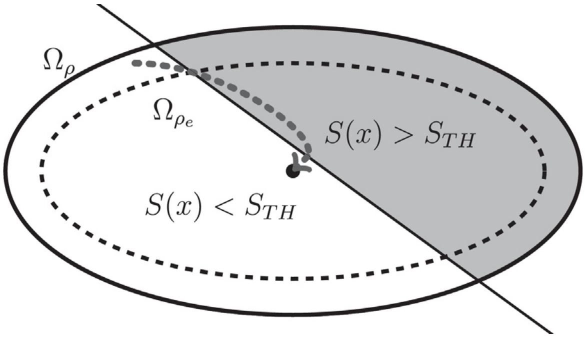

Fig. 3. Example of level sets Ω_ρ and Ω_{ρ_e} partitioned based on $S(x)$. The origin, represented by a black dot at the center of the level sets, is within the safety zone. The black ellipse represents the boundary of Ω_ρ. The dotted ellipse represents the boundary of Ω_{ρ_e}. The dotted dark gray line represents an example trajectory that starts within the safety zone but leaves it as it moves into Lyapunov level sets with lower upper bounds on the Lyapunov function until it re-enters the safety zone as it approaches the origin.

or $V(x)$ upon which the constraints of Eqs. (6e) and (6g) are based and therefore, when Eq. (6e) and/or (6g) is enforced concurrently with Eq. (6f), the Safeness Index-based MPC is not guaranteed to have a feasible solution that satisfies all of these constraints (however, due to the definition of $S(x)$ without reference to a controller, even in the absence of Eqs. (6e) and (6g), there is no guarantee that a feasible solution meeting the input constraints and following the process dynamics exists, meaning that under any control design, including Safeness Index-based MPC, the state may leave the safety zone). As a result, there is no control law guaranteed to maintain the closed-loop state within the safety zone at all times that can be taken advantage of for defining stability constraints for the MPC. Because no alternative stabilizing controller with which to design the stability constraints is obvious from the definition of the safety zone, the Lyapunov-based stability constraints of Eqs. (6e) and (6g) are used in the Safeness Index-based MPC due to their ability to guarantee closed-loop stability and recursive feasibility of the optimization problem of Eq. (6) when Eq. (6f) is not applied.

Fig. 3 clarifies why feasibility of the Safeness Index-based MPC can be problematic. Specifically, $h(x)$ implemented in sample-and-hold is guaranteed to be a feasible solution to the Safeness Index-based MPC design when $S(x) > S_{TH}$ so that the constraint of Eq. (6f) is not applied (because the MPC of Eq. (6) then reduces to the MPC design of Eqs. (3) and (5) for which Heidarinejad et al. (2012) has proven feasibility of this solution). However, despite that a feasible solution exists when the constraint of Eq. (6f) is removed, when it is enforced, $h(x)$ implemented in sample-and-hold may not cause Eq. (6f) to be satisfied because it is guaranteed to decrease the Lyapunov function value between two sampling periods of the prediction horizon, but as shown in Fig. 3, decreasing the Lyapunov function value does not necessarily correspond to maintaining the process state within the safety zone, depending on the shape of the safety zone. Specifically, Fig. 3 shows a potential state trajectory (the dotted dark gray trajectory in the figure) initiated from a point within Ω_ρ but outside Ω_{ρ_e}, where the state is being driven to the origin over time (for the purposes of illustrating that decreasing the value of $V(x)$ under $h(x)$ does not correspond to maintaining the state within the safety zone, this trajectory can be considered to be the trajectory under $h(x)$ meeting Assumption 1 implemented in sample-and-hold). The state is driven outside the safety zone by the control actions on its way to the origin despite that both the initial state and the origin are within the safety zone. This shows that $h(x)$ implemented in sample-and-hold, which is the feasible solution to all constraints except Eq. (6f), cannot guarantee that Eq. (6f) is satisfied as well and thus, an alternative characterizable control action must be applied when the Safeness Index-based MPC becomes infeasible (in accordance with Desirable Property 4). Albalawi et al. (2017d) develops an implementation strategy for the Safeness Index-based MPC design that applies the Safeness Index-based MPC solution when that solution is feasible at t_k or $h(x(t_k))$ when it is not. In this case, stability properties (a)–(c) are obtained for a nonlinear process under this implementation strategy with property (b) signifying that the closed-loop state can always be driven into the safety zone in finite time when the state leaves this region.

Despite the fact that the safety zone is not a forward invariant set under the Safeness Index-based MPC and that the constraint of Eq. (6f) can cause infeasibility of the control design, the constraint plays an important role in enhancing process safety. Specifically, though it may not be possible to meet the constraint in every sampling period, there may be cases in which an MPC design with the form of Eq. (6) but without the constraint of Eq. (6f) would find that the objective function is maximized within a region in Ω_ρ where $S(x)$ would be greater than S_{TH}. The implication of this is that the MPC may purposefully drive the process state through that region in Ω_ρ (in both the case of a tracking MPC that is driving the process state to the steady-state when initiated off of the steady-state or in the case of an MPC with a general objective function operating a process in a time-varying fashion) or, in the case that MPC with a general objective function is utilized and the process state can be maintained within the region where the objective function is maximized subject to the input constraints and process model, the MPC may operate the process for long periods of time in this region that is outside the safety zone (in Albalawi et al., 2017d, a process example that compares the state trajectories with respect to the safety zone under an MPC without Safeness Index-based constraints and under an MPC with Safeness Index-based constraints demonstrates the ability of Safeness Index-based constraints to cause an MPC to compute control actions that maintain the process state in the safety zone when it would not do so without those constraints). Thus, even if the process state does exit the safety zone for finite periods of time during normal process operation for a process operated under Safeness Index-based MPC, the Safeness Index-based constraints may aid in keeping it within the safety zone for much more of the time than it otherwise would be within the safety zone and will ensure that the state is driven back into the safety zone in finite time when it exits this region, which also may not otherwise occur.

3.3.3. Safeness Index-Based MPC: special $S(x)$ form for stability, feasibility, and safety-related guarantees

An important question is whether it is acceptable for the process state to exit the safety zone for finite periods of time as described above. The answer to this depends on the definitions of $S(x)$ and of S_{TH} developed by engineers for a specific process. For example, if an engineer sets S_{TH} conservatively enough that based on closed-loop simulations of the process state under the Safeness Index-based MPC in the presence of bounded process disturbances, the engineer determines that it is unlikely that during normal process operation, the closed-loop state will move far enough from the safety zone when the process is operated under the Safeness Index-based MPC to activate the safety system or to cause incidents, it may be acceptable to allow the process state to exit the safety zone for finite periods of time. In addition, because the state can be driven into $\Omega_{\rho_{\min}}$ (by, for example, $h(x)$ implemented in sample-and-hold) which is within the safety zone and maintained there thereafter by the definition of $\Omega_{\rho_{\min}}$ in Definition 1, engineers may try tuning S_{TH} on-line (assuming Assumption 2 holds for each S_{TH} tested) by trying different values of S_{TH} within the Safeness Index-based MPC and observing whether the process state is maintained within a range of states that are not associated with incidents or safety system activation under normal process operation, knowing that the control action available can bring the state back into a safe operating region ($\Omega_{\rho_{\min}}$) if the state appears to be headed further outside of the safety zone than desired for a given S_{TH}. There may also be cases in which engineers develop S_{TH} to try to maintain the state within the safety zone defined by S_{TH} as often as possible but are willing to accept the state going outside this region due to the potential economic gains of not setting a more conservative threshold; this may be the case, for example, if long periods of operation at high temperature may damage the reactor materials but short-term temperature increases are not expected to be problematic. However, $S(x)$ and S_{TH} for some processes may be designed such that S_{TH} represents a hard threshold on the Safeness Index (i.e., engineers consider that the process state should under no circumstances exit the safety zone to avoid incidents and safety system activation). In these cases, a special functional form of $S(x)$ can be developed for which the Safeness Index-based MPC of Eq. (6) guarantees not only stability properties (a)–(c), but also guarantees that $h(x)$ implemented in sample-and-hold is a feasible solution at every sampling time and that once the state enters the safety zone, it will not leave it (even in the presence of bounded disturbances). The special form of $S(x)$ required is $S(x)=V(x)$ (e.g., $S(x)=x^TP\,x$ for $V(x)=x^TP\,x$, for a positive definite matrix P). In this case, S_{TH} has to be a value that is more conservative than the value $S_{TH,d}$ that defines the boundary of the safe operating region (i.e., it is desired that $S(x)\leq S_{TH,d}$ for all times after the closed-loop state enters the safe operating region). Because $S(x)=V(x)$, the conservatism in S_{TH} must be such that for a nonlinear process operated under the Safeness Index-based MPC, when $x(t_k)\in\Omega_{S_{TH}}$, then $x(t_{k+1})\in\Omega_{S_{TH,d}}$. In addition, by Assumption 2 and the definitions of Ω_ρ and Ω_{ρ_e}, it is necessary that $\rho_{\min}\leq S_{TH}\leq\rho_e$ and $S_{TH}<S_{TH,d}\leq\rho$.

The reason that this special formulation of $S(x)$ conquers the feasibility issues of the standard Safeness Index-based MPC design of Eq. (6) with a general $S(x)$ and is guaranteed to maintain the closed-loop state within the region where $S(x)\leq S_{TH,d}$ when the MPC of Eq. (6) with a general $S(x)$ cannot do this is because the special formulation relates $S(x)$ to $V(x)$ and $h(x)$, therefore guaranteeing that $h(x)$ implemented in sample-and-hold is a feasible solution of the Safeness Index-based constraint (as well as the other constraints as mentioned above) and maintains the process state within the region where $S(x)\leq S_{TH,d}$ when the state enters that region. Despite these guaranteed feasibility and stability properties of the Safeness Index-based MPC with $S(x)=V(x)$ and its ability to not only drive the process state into a safe operating region but to maintain it there, the requirement that $S(x)$ by a Lyapunov function where S_{TH} places the Lyapunov level set defined by $S(x)$ within the safe operating region may sacrifice economic performance and therefore may not be a desirable functional form for $S(x)$ when there is not a need to set $S(x)=V(x)$ in order to prevent incidents and safety system activation. When $S(x)$ is set to $V(x)$, this essentially requires that based on all considerations in Section 3.1, a safe operating region must be characterized and then the largest level set of the Lyapunov function for the nominal nonlinear process of Eq. (1) under $h(x)$ within that region may be chosen as the region $\Omega_{S_{TH,d}}$. Such a region may be much smaller than the full safe operating region (which can be understood through analogy with Fig. 2 in which an assumed level set of the Lyapunov function is much smaller than the white triangular safe operating region), and restricting process operation to smaller regions can sacrifice economic performance. Under no circumstances should operational safety be sacrificed for economic performance, but the designs of $S(x)$ and S_{TH} should not be so conservative that economic performance is unnecessarily sacrificed (in accordance with Desirable Property 3).

3.3.4. Safeness Index-Based MPC: extracting design principles from other safety-based MPC designs

An important question that has not been addressed so far in the literature on Safeness Index-based MPC is whether there are methods for adjusting the rate at which the closed-loop state re-enters the safety zone when it leaves it (i.e., alternative formulations of the MPC of Eq. (6) to be used when $S(x(t_k))>S_{TH}$ to potentially achieve faster rates of convergence of the closed-loop state back into the safety zone have not been analyzed). The motivation for looking at this issue is twofold: (1) The ability to adjust the rate at which the state re-enters the safety zone may affect the value of S_{TH} chosen; for example, if a Safeness Index-based MPC formulation could be developed for which the time that the state spends outside the safety zone when it exits it is less than under the MPC of Eq. (6), it may be possible to set S_{TH} less conservatively; and (2) The rate at which the state re-enters the safety zone for the MPC of Eq. (6) may be dependent on the objective function. To see this latter point, it is noted that when $S(x(t_k))>S_{TH}$, the MPC is guaranteed to be feasible at each sampling time with $h(x)$ in sample-and-hold as the feasible solution, and the constraint with the role of guaranteeing that the state is driven back into the safety zone in finite time is Eq. (6g); however, this constraint requires only that the amount by which the MPC-computed control action would decrease the Lyapunov function value along the predicted state trajectory (to cause the state to approach $\Omega_{\rho_{\min}}$ which is within the safety zone) be at least as much as $h(x(t_k))$ would decrease it at t_k. This means that in a worst case, the length of time before the state re-enters the safety zone is given by the following definition which follows from the results of Heidarinejad et al. (2012) and is defined in Alanqar et al. (2017a) for an MPC with the same form as the MPC of Eq. (6) when $S(x(t_k))>S_{TH}$ (i.e., only Eqs. (6a–6e) and (6g) may be applied).

Definition 2. Consider the process of Eq. (1) operated under $h(x)$ meeting Assumption 1 implemented in sample-and-hold or under the MPC of Eq. (6) based on $h(x)$ meeting Assumption 1 (or under a combination of the control actions computed by these control laws such that at every sampling time, a control action from one of the two control laws is applied). Then, the worst-case length of time t_{WC} that the process state can spend outside of the safety zone when $S(x(t_k))>S_{TH}$ and $\rho_{\min}$ is defined as in Definition 1 is obtained from the worst-case upper bound on the time derivative of the Lyapunov function in Heidarinejad et al. (2012) (i.e., $\dot{V}=-\epsilon_w/\Delta$, where $\epsilon_w>0$ is a constant related to Δ, θ, ρ_s, and the properties of f) and the worst-case initial and final values of V outside the safety zone (ρ and $\rho_{\min}$, respectively), and is $t_{WC}=\Delta(\rho-\rho_{\min})/\epsilon_w$.

The objective function and the shape of the safety zone will play important roles in the rate at which the state re-enters the safety zone. If the optimal input trajectory, for example, is a path outside the safety zone where the objective function is maximized (but where the constraints are met), then the MPC will not seek to drive the process state back into the safety zone immediately. However, because the safety zone may have an irregular shape, it is difficult to analyze how the objective function, disturbances, and constraints may contribute to the rate at which the state re-enters the safety zone.

Despite the difficulties of being able to predict the amount of time that the state will actually spend outside of the safety zone when it exits it under the MPC of Eq. (6), it is reasonable to expect that there may be methods for adjusting the MPC to try to obtain different rates of convergence of the state to the safety zone than are obtained with Eq. (6). Albalawi et al. (2016) examines several different formulations of MPC's that for safety reasons drive the state from one operating region to a safer one, and analyzes the impacts of the formulations on the rates at which the MPC's do this. However, Albalawi et al. (2016) does not define the safe operating regions with respect to a Safeness Index, but instead assumes that they are level sets of a Lyapunov function in state-space. From the discussions of $S(x) = V(x)$ as a special case of a Safeness Index formulation, however, it can be inferred that the principles behind the designs in Albalawi et al. (2016) may be extended to Safeness Index-based MPC to develop formulations with various rates of approach back to the safety zone. Below, we present the essential features of the techniques by which the four formulations in Albalawi et al. (2016) drive the state to a safe level set of operation at various rates, and we subsequently analyze how these principles may be used to develop Safeness Index-based MPC designs with the flexibility to adjust the rate of approach of the process state back into the safety zone when it leaves that set. The formulations will be presented in terms of $S(x)$ for consistency with the notation used throughout this tutorial, but when referring to the properties developed in Albalawi et al. (2016), it should be understood that the assumption in that work is that $S(x) = V(x)$ (therefore, any mention of the state being outside a safe operating region for the formulations in Albalawi et al. (2016) implies that it was initiated outside of the safe operating region because like the MPC designs with $S(x) = V(x)$ mentioned in the prior section, those in Albalawi et al. (2016) guarantee that once the state enters a safe operating region, it will not leave it as long as S_{TH} is defined such that $x(t_k) \in S_{TH}$ implies $x(t_{k+1}) \in S_{TH,d}$). The formulations are as follows:

Formulation 1 (referred to as Scheme 1 in Albalawi et al. (2016)): This formulation utilizes the contractive constraint (Eq. (6g)) to ensure that the closed-loop state is driven from a region outside of a safe level set of operation into that safe level set in finite time.

Formulation 2 (referred to as Scheme 2 in Albalawi et al. (2016)): This formulation utilizes a hard region constraint to require that the state be within a safe operating region by a certain time in the prediction horizon (though it may be outside of that operating region before the specified time). The ability to satisfy such a constraint depends on the prediction horizon length and is difficult to guarantee in the presence of disturbances since the formulation in Albalawi et al. (2016) does not utilize the contractive constraint.

Formulation 3 (referred to as Scheme 3-1 in Albalawi et al. (2016)): This formulation utilizes the contractive constraint to guarantee that the closed-loop state is driven into a safe level set in finite time from a region outside of the safe level set, but in addition incorporates a slack variable expressing the difference between the value of $S(x)$ along the predicted state trajectories and the threshold value $S_{TH,d}$ that can be highly penalized in the objective function to encourage the MPC to compute control actions that drive the state into the region where $S(x) \le S_{TH,d}$ potentially more quickly than it otherwise might if the objective function was not modified when the state was outside of the safe operating region. Specifically, this MPC formulation computes not only a piecewise-constant input trajectory but also a piecewise-constant trajectory for the slack variable $s(t)$ that maximizes the objective function

$$\int_{t_k}^{t_{k+N}} [L_e(\tilde{x}(\tau), u(\tau)) - a_L s(\tau)^2] d\tau \tag{8}$$

where $a_L > 0$ is the penalty on the slack variable. The constraints are similar to those of the MPC of Eq. (6) when $S(x(t_k)) > S_{TH}$, but the following constraint also must be satisfied during the time that the state is outside of the safe operating region:

$$S(\tilde{x}(t)) + s(t) \le S_{TH,d}, \quad \forall \ t \in [t_k, t_{k+N}) \tag{9}$$

where $s(t) \le 0, \forall\, t \in [t_k, t_{k+N})$, if $S(x(t_k)) > S_{TH,d}$.

Formulation 4 (referred to as Scheme 3-2 in Albalawi et al. (2016)): This formulation utilizes the contractive constraint to drive the closed-loop state into a safe level set in finite time, but like Formulation 3, it adds an auxiliary optimization variable (which is a piecewise-constant optimization variable K_c that unlike $s(t)$ is not required to have the same sampling period as $u(t)$ and may provide greater flexibility in adjusting the speed of the approach to the safe operating region when it does not). K_c does not appear in the objective function but only in some constraints of the optimization problem (unlike $s(t)$, which appears in the objective function of Formulation 3, and because it appears in the objective function, care must be taken in specifying the value of a_L to be sufficiently large so that the optimal solution to the Formulation 3 optimization problem does not contain s with a large magnitude since that would allow the predicted state to evolve in a large region outside of the region where $S(\tilde{x}(t)) \le S_{TH,d}$ according to Eq. (9)). The constraints related to K_c in Formulation 4, which are applied when the state is outside of the safe operating region, are:

$$K_c(t) \ge 0, \ \forall \ \ t \in [t_k, t_{k+N}) \tag{10a}$$

$$S(\tilde{x}(t)) \le \tilde{\rho}(t), \ \forall \ \ t \in [t_k, t_{k+N}) \tag{10b}$$

$$\frac{d\tilde{\rho}}{dt} = K_c(t)(S_{TH,d} - \tilde{\rho}(t)) \tag{10c}$$

$$\tilde{\rho}(t_k) = S(x(t_k)), \quad \text{if} \ \ S(x(t_k)) > S_{TH,d} \tag{10d}$$

These constraints allow the optimization variable K_c to be chosen to decrease $\tilde{\rho}$ (the upper bound on the Lyapunov function along the predicted state trajectory since Albalawi et al. (2016) assumes $S(x) = V(x)$ in Eq. (10b)) throughout every sampling period of the prediction horizon (where the process dynamics also affect the value of K_c that can be chosen) to seek to maximize the following objective function:

$$\int_{t_k}^{t_{k+N}} [L_e(\tilde{x}(\tau), u(\tau)) - \phi(S_{TH,d} - \tilde{\rho}(\tau))] d\tau \tag{11}$$

where $\phi(S_{TH,d} - \tilde{\rho}(\tau))$ represents a penalty function that takes $S_{TH,d} - \tilde{\rho}(\tau)$ as an argument, and therefore may be, for example, a scalar-valued quadratic function of its argument. The other constraints of Formulation 4 are similar to those of Eq. (6) when $S(x(t_k)) > S_{TH}$.

Because Formulations 1–4 were developed for the case that safe operating regions are Lyapunov level sets, it is straightforward to consider modifying Eq. (6) when $S(x) = V(x)$ and $S(x(t_k)) > S_{TH}$ so that it takes the form of Formulation 1, 2, 3, or 4 until the state enters $\Omega_{S_{TH,d}}$. In such cases, the results from Albalawi et al. (2016) regarding the rates of approach of the state to the safe operating region would hold. Specifically, for nominal operation and a sufficiently long prediction horizon, Formulation 2 can drive the state into $\Omega_{S_{TH,d}}$ by a specific time in the prediction horizon (it also guarantees boundedness of the closed-loop state in Ω_ρ and a feasible control action $h(x)$ in sample-and-hold at each sampling time in the absence of disturbances). Formulations 1, 3, and 4, unlike Formulation 2, have provable closed-loop stability and feasibility properties even in the presence of disturbances (i.e., the MPC formulations drive the state into a safe operating region in finite time and $h(x)$ in sample-and-hold is a feasible solution at every sampling time), but are only able to guarantee that the state is driven into $\Omega_{S_{TH,d}}$ within t_{WC}. However, though Formulation 1 is similar to Eq. (6) with $S(x(t_k)) > S_{TH}$, meaning that the primary goal of the controller is to optimize the objective function during the approach to the safe operating region and not to necessarily approach the safe operating region quickly, the penalties in the objective functions of Formulations 3 and 4 can be chosen to weight L_e and the penalty term in such a way that the state may enter the safe operating region in less time than without the penalty terms (i.e., the penalty term may need to be significantly larger in magnitude than L_e because the maximization of L_e does not necessarily occur within $\Omega_{S_{TH,d}}$, so when more weight is given to L_e, the predicted state may take a trajectory that does not enter $\Omega_{S_{TH,d}}$ quickly). With disturbances, it is difficult to tell whether the actual state will enter $\Omega_{S_{TH,d}}$ as quickly as the predicted state does, but Formulations 3 and 4 provide the flexibility through the penalty term of the objective function to try to adjust the rate of approach of the state to $\Omega_{S_{TH,d}}$, whereas Formulation 1 does not. Albalawi et al. (2017a) elucidates the relationship between the rate of approach of the state to the safe operating region and the gain K_c by developing a hard decreasing exponential upper bound on Eq. (10b) and noting that if K_c can be chosen to allow $\tilde{\rho}$ to decrease at the rate of that hard upper bound, then K_c is chosen to achieve a specific rate of approach of the (predicted) state to a safe operating region. Albalawi et al. (2017a) also highlights that having an adjustable penalty term in the objective function can be helpful in the case that a tracking MPC is controlling the process and the state must approach a safe operating region more quickly than it would with the weighting matrices Q_T and R_T used under normal operating conditions. It would be difficult to determine a manner to adjust these weighting matrices to obtain the required rate of approach of the state to the safe operating region, but the penalty term can be more easily tuned.

Because Formulations 1–4 have been written in terms of $S(x)$ above (though for the case that $S(x)$ is assumed to be $V(x)$), we can consider the implications of applying similar formulations in place of Eq. (6) when $S(x(t_k)) > S_{TH}$ but $S(x) \neq V(x)$. The primary principles of the results described for the case that $S(x) = V(x)$ above would hold. Specifically, if a hard constraint on the time before the state re-enters the safety zone were utilized (as in Formulation 2), then the optimization problem may not be feasible in the presence of disturbances and without a sufficiently long prediction horizon. If Eq. (6) were used as is (resembling Formulation 1), there would be no penalty term in the objective function to change the rate of approach of the state to the safe operating region when $S(x(t_k)) > S_{TH}$, whereas if it was augmented by Eqs. (8) and (9) when $S(x(t_k)) > S_{TH}$ (to be like Formulation 3) or by Eqs. (10) and (11) when $S(x(t_k)) > S_{TH}$ (to be like Formulation 4), it would have a penalty term that could be tuned to attempt to speed the rate of approach. An important point in attempting to speed the rate of approach by adding constraints and penalty terms in the objective function is that even if the predicted state is driven back into the safe operating region more quickly than without the modified formulation, the actual state trajectory may not be. The case that $S(x) \neq V(x)$ for designs following Formulations 1, 3, and 4 is particularly interesting in this regard, because though the constraint of Eq. (6g) guarantees that the closed-loop state is driven to a lower level set throughout every sampling period even with disturbances, the shape of the safety zone may be such that moving to a lower level set moves the state further from the safety zone instead of closer (note that this cannot happen when $S(x) = V(x)$ because in that case, driving the state into a level set with a lower upper bound on the Lyapunov function means that the state moves closer to the safety zone). Fig. 4 demonstrates this concept by showing that the shape of the safety zone may be such that the state is closer to the safety zone when the value of $V(x)$ at a given state is larger than when it is smaller. This means that disturbances can play an important role in causing the state to take longer to re-enter the safety zone than it would without disturbances. It also means that if an MPC with a penalty term reflecting the closeness of the state to the safety zone like Formulation 3 or 4 was aware of the disturbances, it might choose significantly different input trajectories than if it is not (these latter two sentences hold for the case that $S(x) = V(x)$ as well). The implication of this is that it is difficult to estimate *a priori* the length of time before the state re-enters the safety zone when the process is operated under designs like Formulations 1, 3, or 4. Another consideration when $S(x) \neq V(x)$ is that in Formulation 4 when $S(x(t_k)) > S_{TH}$, the constraint of Eq. (10b) is not guaranteed to be satisfied (i.e., it is like the constraint of Eq. (6f)). Therefore, the formulation of Eq. (6) with modifications according to Formulation 4 may become infeasible so an implementation strategy (for example, using $h(x)$ in sample-and-hold) might be needed when the formulation becomes infeasible as the state re-enters the safety zone, or other methods of modifying the optimization problem of Eq. (6) when $S(x(t_k)) > S_{TH}$ like adding a penalty term on the difference between S_{TH} and $S(\tilde{x})$ in the objective function may be considered.

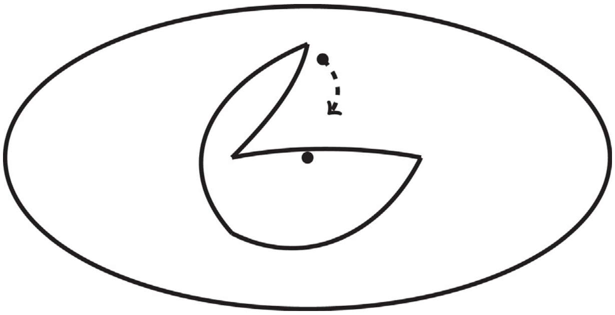

Fig. 4. Example of an irregularly shaped safety zone within an ellipse-shaped stability region. The origin is contained within the safety zone. The initial state for the dashed state trajectory is closer to the safety zone (in terms of the distance between any the point in the state trajectory and the closest point in the safety zone) than the state is after the state has moved into a region where the upper bound on the Lyapunov function has decreased.

Because it may be difficult for Safeness Index-based MPC to determine the amount of time that the state will spend outside of the safety zone when it leaves the safety zone, it is beneficial to be able to upper bound the time (e.g., Definition 2) to aid in developing thresholds on $S(x)$ and understanding the worst-case operating conditions to evaluate the potential for incidents for a closed-loop process. This leads to the statement of the following desirable property of a control design for maintaining process safety.

Desirable Property 5. The rate at which the MPC can drive the closed-loop state back into a desired operating region when the state exits such a region should be characterizable.

3.3.5. Safeness Index-Based MPC: identifying and evaluating methods for overcoming infeasibility limitations

Feasibility has been shown to be an issue for the optimization problem of Eq. (6), rooted in the formulation of the Safeness Index as a general function not tied to a control design, and therefore it is important to recognize tuning parameters of the optimization problem that may make it more likely to be feasible. One important tuning parameter is the sampling period Δ, because control actions are held for this length of time. When Δ is shorter, the MPC computes a new input more frequently and therefore may have greater flexibility to alter the process dynamics to try to steer the predicted state away from the region where $S(x) > S_{TH}$. Though feasibility is not an issue when $S(x) = V(x)$, having a shorter sampling period allows $\Omega_{\rho_{\min}}$ to be made smaller. Since $\rho_{\min}$ provides a lower bound on S_{TH} and $S_{TH,d}$ for the case that $S(x) = V(x)$ as discussed above, Δ must be sufficiently small to allow $\rho_{\min}$ to be small enough that S_{TH} can be set to the value it needs to take to ensure that the state never leaves $S_{TH,d}$. Though in general, the sampling period should not be shorter than the time it takes to solve the optimization problem of Eq. (6) (especially when L_e is an economics-based objective function in which case optimality of the solution returned by the MPC of Eq. (6) may be important to production goals), the Safeness Index-based MPC may require a significant computation time when there are tens or hundreds of optimization variables and states as may occur for the practical situations for which the Safeness Index-based MPC was developed to help promote operational safety at on-line plants. To handle com-

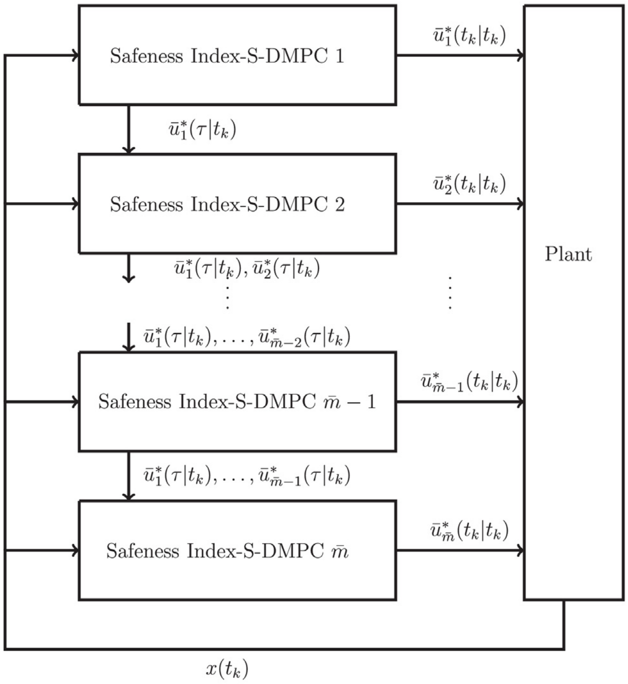
Safeness Index-S-DMPC 1
$\bar{u}_1^*(t_k|t_k)$
$\bar{u}_1^*(\tau|t_k)$
Safeness Index-S-DMPC 2
$\bar{u}_2^*(t_k|t_k)$
$\bar{u}_1^*(\tau|t_k), \bar{u}_2^*(\tau|t_k)$
Plant
$\bar{u}_1^*(\tau|t_k), \ldots, \bar{u}_{\bar{m}-2}^*(\tau|t_k)$
Safeness Index-S-DMPC $\bar{m}-1$
$\bar{u}_{\bar{m}-1}^*(t_k|t_k)$
$\bar{u}_1^*(\tau|t_k), \ldots, \bar{u}_{\bar{m}-1}^*(\tau|t_k)$
Safeness Index-S-DMPC $\bar{m}$
$\bar{u}_{\bar{m}}^*(t_k|t_k)$
$x(t_k)$

Fig. 5. Block diagram of the Safeness Index-S-DMPC scheme.

putation time issues for Safeness Index-based MPC, Albalawi et al. (2017c) has investigated two different distributed control architectures known as sequential Safeness Index-based distributed MPC (Safeness Index-S-DMPC) and iterative Safeness Index-based distributed MPC (Safeness Index-I-DMPC) which may have lower computation times than a centralized Safeness Index-based MPC and may thus be able to use a lower value of Δ. The distributed control designs may have a lower computation time than a centralized design because they solve $\bar{m}$ distributed optimization problems with the same objective function as the centralized optimization problem and similar constraints, but with less decision variables, which is facilitated by assuming values of all inputs except for a subset of m_i inputs within the $i-th$ distributed controller. Results have been developed for the distributed control designs regarding their abilities to maintain feasibility and closed-loop stability, and their ability to drive the closed-loop state into the safety zone and to maintain it within that region, for input-affine nonlinear systems with the form in Eq. (2) (the notation of Eq. (2) will be used in the remainder of this section, though the distributed control designs may be applied to the general class of nonlinear systems of Eq. (1) but without guarantees on the properties mentioned above).

In the sequential distributed control design, $\bar{m}$ controllers are connected via a one-directional communication network such that they communicate in the manner depicted in Fig. 5, which reflects that the controllers are solved in a sequence, with the $i-th$ controller solving for a subset of the set of m control actions contained within $\bar{u}_i$ while assuming a value of the rest of the manipulated inputs in a sense to be clarified below. Specifically, the $i-th$ distributed Safeness Index-based MPC in the sequence (denoted by Safeness Index-S-DMPC i) receives the $i-1$ optimal input trajectories denoted by $\bar{u}_j^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $j = 1, \ldots, i-1$, (where $\bar{u}_j^*(t_q|t_k)$, $q = k, \ldots, k+N-1$, is the piecewise-constant value of $\bar{u}_j$ computed at t_k for the time period $t \in [t_q, t_{q+1})$ in the prediction horizon) computed by the $i-1$ distributed Safeness Index-based MPC's before it in the sequence and communicates these trajectories in addition to its own solution $\bar{u}_i^*(t|t_k)$, $t \in [t_k, t_{k+N})$, to Safeness Index-S-DMPC $i+1$. Safeness Index-S-DMPC i is a modified version of the centralized Safeness Index-based MPC of Eq. (6) in the sense that it solves only for $\bar{u}_i$ and assumes (through additional constraints) that the values of $\bar{u}_j$, $j = 1, \ldots, i-1$, are equal to the received optimal values from the controllers before it in the sequence while it assumes $\bar{u}_j = \bar{h}_j(\tilde{x}(t))$ implemented in sample-and-hold for the rest of the control inputs (where $\bar{h}_j(x)$ is the control law comprised of the components of $h(x)$ corresponding to the components of $\bar{u}_j$). When the process controlled under this sequential distributed Safeness Index-based MPC architecture is of the form of Eq. (2), it is proven in Albalawi et al. (2017c) that feasibility of Safeness Index-S-DMPC 1 guarantees feasibility of the remaining $\bar{m}-1$ controllers in the sequence (as for the centralized Safeness Index-based MPC on which this distributed control design is based, feasibility of Safeness Index-S-DMPC 1 is guaranteed with $\bar{u}_1(t) = \bar{h}_1(\tilde{x}(t))$ implemented in sample-and-hold except when the constraint of Eq. (6f) is applied). In Albalawi et al. (2017c), it is proven that stability properties (a)–(c) hold if the process of Eq. (2) is operated under the combination of the solution of the Safeness Index-S-DMPC when Safeness Index-S-DMPC 1 is feasible and $h(x(t_k))$ when it is not. A sequential distributed MPC design executed in the manner described in Fig. 5 was also developed in Albalawi et al. (2017b) for Formulation 4 described in the prior section for the case that $S(x) = V(x)$ and $x(t_k) \in \Omega_{S_{TH}}$ implying that $x(t_{k+1}) \in \Omega_{S_{TH,d}}$. It was proven to guarantee stability properties (a)–(c) with $h(x)$ implemented in sample-and-hold guaranteed to be a feasible solution at every sampling time and the state being maintained within $\Omega_{S_{TH,d}}$ after it enters it, when θ, Δ, ρ_s, and the properties of $\bar{f}$, b, g_i, and U_i, $i = 1, \ldots, m$, meet certain conditions. When $K_c = 0$, Formulation 4 has similarities to Eq. (6) with $S(x) = V(x)$ and a sufficiently small S_{TH}, and therefore the feasibility and stability guarantees just described can be made for a sequential distributed design for the MPC of Eq. (6) when $S(x) = V(x)$.

The iterative distributed control design, unlike the sequential distributed control design, involves the simultaneous solution of $\bar{m}$ controllers at one time, where the $i-th$ iterative Safeness Index-based distributed MPC (denoted by Safeness Index-I-DMPC i), $i = 1, \ldots, \bar{m}$, assumes a value for all control actions except for the m_i control actions for which it solves, as shown in Fig. 6. The distributed controllers in this design do not share their solutions until after all $\bar{m}$ controllers have computed them (and thus the $i-th$ controller initially assumes that $\bar{u}_j$, $j \in \{1, \ldots, \bar{m}\}$ except $j = i$, are set to $\bar{h}_j(\tilde{x}(t))$ implemented in sample-and-hold), but after all controllers solve (which constitutes an iteration of the distributed control algorithm), the controllers may exchange solutions and re-solve the optimization problem, where the $i-th$ controller assumes that all control actions $\bar{u}_j(t)$ for $j \in \{1, \ldots, \bar{m}\}$ except $j = i$, are set to the optimal values $\bar{u}_{j,c-1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, returned by the distributed controllers except the $i-th$ at the prior iteration during this re-solution of the optimization problem (where the subscript $c > 0$ signifies the iteration of the algorithm from which the input trajectory was obtained). The $i-th$ distributed MPC solves an optimization problem like that of Eq. (6) except requiring that the inputs except the $i-th$ are set according to the strategy just described. In addition, Albalawi et al. (2017c) replaces the constraint of Eq. (6g) with the following constraint for the $i-th$ distributed controller:

$$\begin{aligned}&\frac{\partial V(x(t_k))}{\partial x} g_i(x(t_k))\bar{u}_i(t_k) \le \frac{\partial V(x(t_k))}{\partial x} g_i(x(t_k))\bar{h}_i(x(t_k)),\\ &\text{if } \; x(t_k) \in \Omega_\rho / \Omega_{\rho_e} \;\text{ or }\; t_k > t_s \;\text{ or }\; S(x(t_k)) > S_{TH}\end{aligned} \tag{12}$$

Eq. (6f) can cause feasibility issues as in the centralized Safeness Index-based MPC, and Eq. (6e) can as well for the iterative distributed design when $c > 1$ because there is no guarantee that there exists a $\bar{u}_i$ that can meet the input constraints for which Eq. (6e) can be met in the ith controller with the rest of the inputs set to their optimal values returned by the other $\bar{m}-1$ distributed controllers

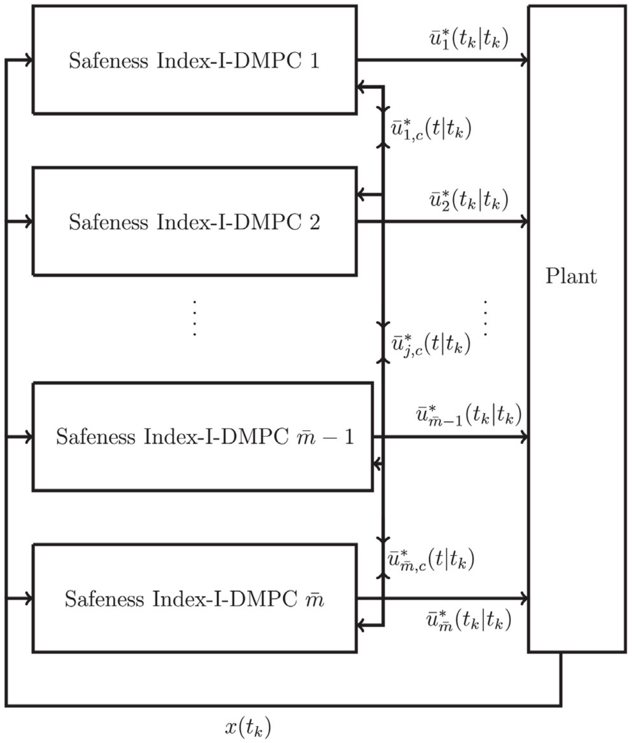
Safeness Index-I-DMPC 1
Safeness Index-I-DMPC 2
Safeness Index-I-DMPC $\bar{m}-1$
Safeness Index-I-DMPC $\bar{m}$
Plant
$\bar{u}_1^*(t_k|t_k)$
$\bar{u}_{1,c}^*(t|t_k)$
$\bar{u}_2^*(t_k|t_k)$
$\bar{u}_{j,c}^*(t|t_k)$
$\bar{u}_{\bar{m}-1}^*(t_k|t_k)$
$\bar{u}_{\bar{m},c}^*(t|t_k)$
$\bar{u}_{\bar{m}}^*(t_k|t_k)$
$x(t_k)$

Fig. 6. Block diagram of the Safeness Index-I-DMPC scheme.

at the prior iteration. Therefore, an implementation strategy was developed in Albalawi et al. (2017c) that checks the values of $V(x)$ and $S(x)$ along the nominal predicted state trajectories under the set of control actions returned by all $\bar{m}$ distributed controllers at iteration c and only performs iteration $c+1$ if the predicted state is maintained within Ω_{ρ_e} and the safety zone (other termination criteria for the iterative design like the maximum number of iterations should also not be met if another iteration is performed). This implementation strategy guarantees that for $c>1$, every distributed controller has a feasible solution. When the checks on $V(x)$ or $S(x)$ or the termination criteria indicate that the next iteration should not be performed, $h(x(t_k))$ is applied if $c=1$, or the solution of iteration $c-1$ is applied if $c>1$. This implementation strategy guarantees that stability properties (a)–(c) are satisfied for the system of Eq. (2) operated under the iterative distributed control design implementation strategy. Albalawi et al. (2017b) develops a similar iterative design and implementation strategy for Formulation 4 when $S(x)=V(x)$ and S_{TH} is sufficiently small that guarantees that stability properties (a)–(c) are satisfied, that there is a feasible solution at every iteration performed, and that the state never exits $\Omega_{S_{TH,d}}$ once it enters it, assuming the conditions on $V(x)$ and $S(x)$ and the termination criteria are checked at the end of every iteration. Due to the similarities between that control design with $K_c=0$ and the Safeness Index-I-DMPC design with $S(x)=V(x)$, the latter also obtains those properties.

An important point with regard to the distributed architectures is that though one of the motivations for their development was to attempt to lower Δ to enhance the potential for feasibility of the optimization problem, feasibility remains an issue with the distributed control designs. In fact, more considerations may need to be checked to guarantee feasibility than in the centralized case, as shown in the implementation strategy of the iterative design that requires the values of $V(x)$ and $S(x)$ to be checked along the predicted state trajectories to guarantee feasibility of all iterations $c>1$, instead of only the value of $S(x)$ as required in the sequential control design. This indicates that though Δ may be able to be decreased through a distributed control design to give more flexibility to the MPC to alter the state trajectory through more frequently adjusted inputs, the distributed control designs create new feasibility issues as well. The sequential or iterative distributed control designs with a general $S(x)$ may be less likely to be feasible than the centralized control architecture (for the same Δ used in each) due to both the lack of knowledge of each distributed controller of the optimal solution of all other controllers and the fact that trying to satisfy the requirement of Eq. (6f) with only a subset of the available control actions within the $i-th$ distributed controller (since $m_i<m$) may provide less flexibility to the MPC for computing control actions to satisfy this constraint. Therefore, Albalawi et al. (2017c) recommends considering the likelihood that all $\bar{m}$ sequential and iterative Safeness Index-based distributed MPC's will have the flexibility to satisfy the constraint of Eq. (6f) during the partitioning of the inputs between all $\bar{m}$ input vectors. Also, because feasibility of the sequential design when $S(x)\neq V(x)$ depends on feasibility of Safeness Index-S-DMPC 1, the partitioning of the control actions into $\bar{u}_1$ in that case should give the controller significant flexibility in affecting the process state trajectory with the inputs in $\bar{u}_1$. However, for large-scale nonlinear process systems with coupled dynamics, it may be difficult to analyze the impact of each u_i, $i=1, \ldots, m$, on the states when seeking to partition the states between the various input vectors (and also interactions between the states when various u_i, $i=1, \ldots, m$, are grouped together to impact the process state predictions within a single distributed controller) without closed-loop simulations. The feasibility issues noted for both the centralized and distributed Safeness Index-based MPC's in Sections 3.3.1–3.3.5 highlight that state-based metric design principles that relate the safety zone to a control law such that it becomes a forward invariant set but without necessarily restricting it to a level set may be beneficial topics for future research (though modified stability constraints based on the controller used to define $S(x)$ in such a case (i.e., not Lyapunov-based) would likely be required to seek to guarantee feasibility and stability), particularly because the level set formulation for $S(x)$ discussed above eliminates feasibility issues of the constraint of Eq. (6f) in both the distributed and centralized control designs because it allows $S(x)$ to depend on the same control law that is feasible for the other constraints. When $S(x)=V(x)$, it should be noted that feasibility of all distributed controllers is guaranteed for the sequential architecture and iterative implementation strategy, and thus the use of a distributed Safeness Index-based MPC design in place of the centralized design may allow Δ to be decreased to decrease $\rho_{\min}$ and S_{TH} if required as mentioned above.

3.4. MPC designs that adjust to faults/process dynamics changes

It has been widely recognized that the performance of an MPC suffers when the process model is a poor representation of the process dynamics, when the state measurements provided to the MPC are inaccurate, or when the actuators fail to implement the control actions computed by the MPC. However, these issues not only cause economic performance degradation, but also affect the ability of the MPC to maintain closed-loop stability and to maintain the process state within a safe operating region. Two general categories of methods for handling actuator/sensor faults and disturbances/dynamics changes in the literature are those that modify the inputs, state measurements, or process model of the MPC when the disturbances or faults occur, and those which assume that some set of inputs or state measurements are unavailable or that the process model must be reconstructed to continue to effectively operate the process, such that a change in the control design itself is needed to handle the faults and disturbances/plant-model mismatch. The first category includes methods that attempt to compensate for actuator or sensor biases or drift with modified control actions or state measurements (e.g., Kettunen et al., 2008; Prakash et al., 2002) or those methods which attempt to compensate for actuator nonlinearities such as stiction by modifying the control actions sent to a valve (Durand and Christofides, 2016; Bacci di Capaci et al., 2017; Srinivasan and Rengaswamy, 2008). It also includes updates of the parameters of a model on-line over time; parameter estimation has been a widely used industrial method for trying to maintain adequate process models for purposes such as determining the economically optimal steady-state for a process to operate at Marlin and Hrymak (1996). MPC's with input rate of change constraints also fall in this category since such constraints may help to reduce actuator wear which might otherwise contribute to actuator faults (Durand et al., 2016; Mhaskar and Kennedy, 2008; Camacho and Bordons, 2007).

The second category of methods mentioned above includes those in which the actuator and sensor issues essentially render the actuators and sensors unusable (for example, an actuator may experience a fault (Abel and Marquardt, 1998), or a sensor or actuator may be taken off-line for preventive maintenance (Lao et al., 2015, 2014b)). It also includes fault-tolerant control using MPC in which an attempt is made to re-configure the control architecture when a fault occurs that renders an actuator unavailable, with the state in the stability region for the new control configuration (Mhaskar, 2006). The method in Lao et al. (2013) falls in this category as well, where an attempt is made, before the time of the fault, to use Lyapunov-based stability constraints to drive the state into a stability region designed without availability of the actuator that is expected to fail. An MPC with a linear empirical model that is updated when significant errors in state predictions occur after disturbances or an actuator fault has also been developed (Alanqar et al., 2017b,c).

The underlying assumption of the works above is that when the correct model and state measurements are utilized in the MPC and the control actions expected are implemented, a well-designed MPC should maintain process closed-loop stability. Some of the designs discussed above develop this assumption more explicitly by providing sufficient conditions under which closed-loop stability is guaranteed (e.g., through Lyapunov stability analysis based on controllers that can be utilized to drive the state to a neighborhood of the origin from a certain region in state-space) even after a sensor or actuator fault occurs. However, as noted in Section 3.2, the region from which closed-loop stability is guaranteed does not necessarily correspond to a safe operating region, unless this is explicitly evaluated through a system-theoretic safety analysis. Therefore, techniques for developing control designs to handle actuator and sensor deficiencies and plant/model mismatch must be extended to MPC designs with system-theoretic safety constraints. This is particularly important considering that system-theoretic constraints on safety may be cast in terms of the process state, so adequate state measurements and reasonably accurate dynamic models are critical for understanding the process evolution with respect to a safe operating region throughout the prediction horizon. Also, for augmenting safety-based control designs with information about unmeasured states that are important to analyzing process operational safety using state estimation, it is necessary to obtain accurate measurements for the states that can be measured on-line.

To date, no work has explicitly addressed changes in the process model or disturbances, sensor faults, or actuator faults in the context of Safeness Index-based MPC. The only results that can be construed as providing initial steps in this direction are results on time-varying safe level sets of operation developed for Formulations 1–4 in Section 3.3.4. Because Section 3.3.4 demonstrated that Formulations 1–4 can provide insights for the development of Safeness Index-based MPC's, we will discuss the results for Formulations 1–4 and then describe their implications for Safeness Index-based MPC.

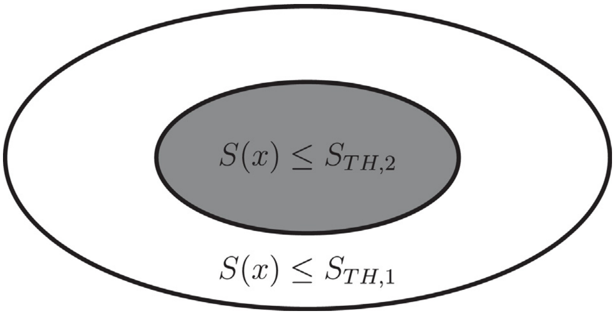

Fig. 7. Example of safe operating regions defined by level sets, where the prior and updated safe level sets of operation are developed around the same steady-state.

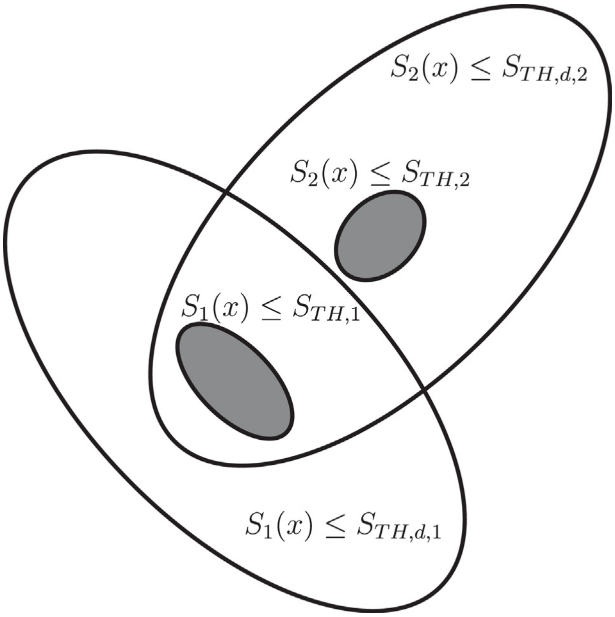

Fig. 8. Example of safe operating regions defined by level sets, where the prior and updated safe level sets of operation are developed around different steady-states, but the safe operating region around the updated steady-state includes the region with the role of $\Omega_{\rho_{\min}}$ around the first steady-state.

The MPC literature with safety-based state constraints based on level sets (i.e., Albalawi et al., 2016, 2017a) has addressed disturbances, changes in the process dynamics, and sensor/actuator faults by looking at how control designs can be modified to handle changes in the safe level set of operation, which can be presented according to the following three principles: (1) Case 1: the prior and updated safe operating regions take the form of level sets that are nested within one another, as demonstrated in Fig. 7; (2) Case 2: the prior and updated safe operating regions take the form of level sets around different steady-states, where the safe operating regions for each steady-state intersect and the region of intersection includes a neighborhood of the first steady-state (i.e., a region that plays the role of $\Omega_{\rho_{\min}}$ for the first steady-state) within the prior safe operating region, as demonstrated in Fig. 8; 3) Case 3: the prior and updated safe operating regions take the form of level sets around different steady-states, where the intersection between the safe operating regions does not include a neighborhood of the origin of the prior steady-state (with the role of $\Omega_{\rho_{\min}}$ for that steady-state), as demonstrated in Fig. 9. Assuming that $S(x) = V(x)$ as in Albalawi et al. (2016, 2017a), these three cases can be cast in terms of the Safeness Index as follows: (1) Case 1: the threshold value on $S(x)$ that defines the boundary of a safe operating region changes from $S_{TH,d,1}$ to $S_{TH,d,2}$ at a certain time (but the functional form of $S(x)$

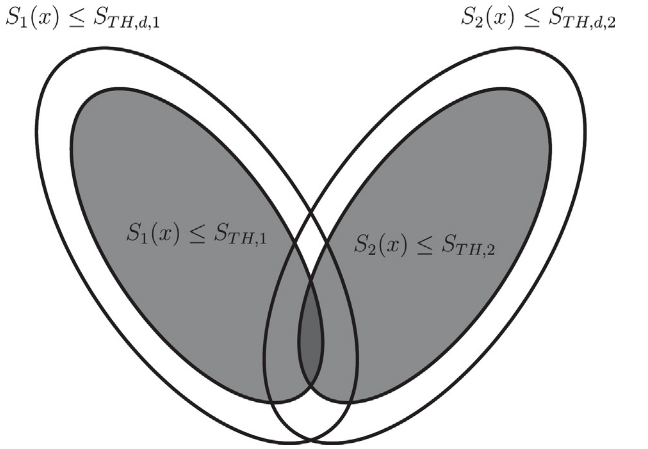

Fig. 9. Example of safe operating regions defined by level sets, where the prior and updated safe level sets of operation are developed around different steady-states, but the safe operating region around the updated steady-state does not include the region with the role of $\Omega_{\rho_{\min}}$ around the first steady-state.

does not change); (2) Case 2: the functional form of $S(x)$ changes, as well as its thresholds defining the boundary of the safe operating region, from $S_1(x)$ to $S_2(x)$ and $S_{TH,d,1}$ to $S_{TH,d,2}$, where the region where $S_1(x) \leq S_{TH,d,1}$ and the region where $S_2(x) \leq S_{TH,d,2}$ are developed around different steady-states, though the region where $S_2(x) \leq S_{TH,d,2}$ around the second steady-state includes the region with the role of $\Omega_{\rho_{\min}}$ around the first steady-state; and 3) Case 3: the functional form of $S(x)$ and its thresholds defining the boundary of the safe operating region change, with the regions where $S_1(x) \leq S_{TH,d,1}$ and $S_2(x) \leq S_{TH,d,2}$ developed around different steady-states, but these regions do not intersect in a region that includes the region with the role of $\Omega_{\rho_{\min}}$ around the prior steady-state. The above three cases can be extended to general $S(x)$ instead of only $S(x) = V(x)$ by considering the following: (1) Case 1 for general $S(x)$ represents that the threshold value on $S(x)$ that defines the boundary of a desirable operating region within the stability region around a given steady-state changes from $S_{TH,1}$ to $S_{TH,2}$; (2) Case 2 for general $S(x)$ represents that the safety zone changes from the region where $S_1(x) \leq S_{TH,1}$ within the stability region around one steady-state to the region where $S_2(x) \leq S_{TH,2}$ within the stability region around another steady-state but that these stability regions both include the region with the role of $\Omega_{\rho_{\min}}$ around the first; (3) Case 3 for general $S(x)$ represents that the stability regions containing the safety zones in which $S_1(x) \leq S_{TH,1}$ and $S_2(x) \leq S_{TH,2}$ do not intersect in a region containing the prior steady-state. The appropriate values of $S(x)$ and S_{TH} that the Safeness Index-based MPC should utilize at a given time are assumed to be communicated to the Safeness Index-based MPC by a safety logic unit (Fig. 10), defined to be a logic unit that performs calculations to determine safe operating regions on-line, such as assessing process data, computing predicted state trajectories from a current state measurement, and determining whether equipment (e.g., actuator or sensor) faults are likely and what the state trajectories will be in such scenarios. It is notable that to this point, no method for reconfiguring the control design due to an actuator fault or obtaining improved state estimates given sensor faults has been looked at for Safeness Index-based MPC, which would be necessary to fully account for such issues (i.e., changing S_{TH} or $S(x)$ may be beneficial, but cannot fully ameliorate the issues with the equipment).

In Albalawi et al. (2016), Case 1 is handled when $S(x) = V(x)$ through Formulations 1–4 described in Section 3.3.4. Specifically, it is assumed that the state is maintained within the prior safe operating region until a switching time t_1, at which the safety logic unit determines that S_{TH} (and $S_{TH,d}$ when $S(x) = V(x)$) must be updated. When it is updated, the principles of Formulations 1–4 are used to drive the state toward the new safe operating region. The rates at which the state will move toward this new safe operating region after the switching time follow the discussion in Section 3.3.4. They extend to the case of general $S(x)$ for Case 1 in the manner described in that section when the state is initially maintained within the stability region around a steady-state, within a safety zone containing the steady-state whenever possible, and then the safety zone is updated so that the state at t_1 may no longer be within the safety zone.

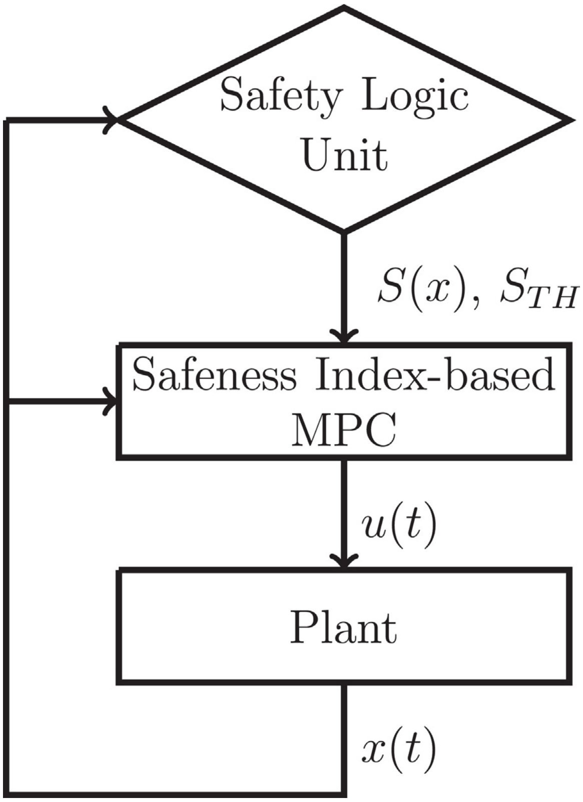

Fig. 10. Schematic depicting flow of information between Safeness Index-based MPC and the safety logic unit which can compute new values of $S(x)$ and/or S_{TH} on-line based on data including a measurement of the current state and communicate them to the MPC.

Cases 2 and 3 have been addressed by the principles in Albalawi et al. (2017a) for a tracking MPC design with the form of Formulation 4 (though the principles hold for MPC with a general objective function) and level set-based operating regions (in that work, stability regions) between which the state is driven. In Case 2, at the switching time t_1, $S(x)$ and the thresholds on it (as well as $V(x)$, $h(x)$, the process model to reflect that the process is then operated around the new steady-state, and the objective function as applicable) are updated in the Safeness Index-based MPC design of Eq. (6) with Eqs. (10) and (11) and $S(x) = V(x)$, but then the updated Safeness Index-based MPC design can be utilized starting at t_1 to drive the process state into the new safety zone in finite time. The same principles apply in the case of a general $S(x)$, and furthermore extend to Formulations 1–3, in the sense that because the stability region around the new steady-state intersects with the prior safety zone (which the state is assumed to be within at t_1 because the state can be driven into this region in finite time according to stability properties (a)–(c) for Eq. (6)), a Safeness Index-based MPC design according to Formulations 1-4 with the constraints written in terms of $S(x)$ as in Section 3.3.4 but updated to reflect operation around the new steady-state can be utilized starting at t_1 because the state is already in the stability region of the new steady-state and therefore the control designs can ensure that the state enters the safety zone around the new steady-state in finite time (though this may not hold for Formulation 2 without a sufficiently long prediction horizon and with disturbances or without handling infeasibility for Formulation 4). Again, the rate considerations of Section 3.3.4 will define the time that it takes the state to move to the new safe operating region. This discussion assumes that the states accessed by the process while transitioning between the safety zones are acceptable from a safety perspective.

In Case 3, there is no guarantee that for any $S(x)$ functional form, or any of the Formulations 1–4, the state can be driven into the new safety zone. This is because the Safeness Index-based MPC designs rely on the fact that $\Omega_{\rho_{\min}}$ is in the safety zone from Assumption 2 to ensure that the state can be driven into the safety zone through the constraint of Eq. (6g) in finite time. When the updated stability region and safe operating region do not contain the origin of the prior stability region and the safe operating region, they do not contain $\Omega_{\rho_{\min}}$ for the prior steady-state, which is the only region in the stability region and safe operating region into which the state can be guaranteed to be driven under the Safeness Index-based MPC. Therefore, while it is possible to consider adjusting the constraints at t_1 as in Albalawi et al. (2017a) to remove all constraints except Eqs. (6b–6d) and add two additional constraints requiring that the state be within the updated stability region after a certain time in the prediction horizon but within the prior stability region before that, there is no guarantee that a feasible solution to this optimization problem exists, especially in the presence of disturbances (even a soft constraint formulation of the optimization problem is not guaranteed to drive the state into the updated stability region). If the state does enter the stability region around the updated steady-state, then Formulation 1, 2, 3, or 4, can be updated to reflect the new steady-state, $S(x)$, and S_{TH}, and the state will be able to be driven to the updated safe operating region in finite time. However, it may not be possible to ever find inputs that drive the state to the intersection of the stability regions such that the updated Safeness Index-based MPC formulation can be applied to drive the state to the updated safe operating region. This is an unsafe scenario in the sense that the state cannot be guaranteed to be driven to a safe operating region, and indicates that changes in $S(x)$ and S_{TH} such that the process is requested to operate around a new steady-state for which the stability region does not contain a neighborhood of the prior steady-state should not be output by a safety logic unit. This shows that the development of the safety logic unit must take this into account so that the unit monitors the plant closely throughout time and tries to adjust the safety zone potentially more frequently than it otherwise would to prevent changes in the operating region from needing to be so drastic that the intersection of the stability regions around the new and prior steady-states does not allow the state to be guaranteed to be driven to a new safe operating region.

This discussion reveals another desirable property of a safety-based MPC as follows.

Desirable Property 6. MPC designs must be able to handle changes in the safe region of operation due to disturbances, equipment faults, and changes in the process dynamics, and to drive the state between safe operating regions in a manner that maintains closed-loop stability and accounts for time constraints on the maximum time that the process state can spend outside a safe operating region.

3.5. Miscellaneous notions of safety tied to process control

For completeness, we mention that several other notions of process safety being maintained through control design in the literature have revolved around adequate control software design (Leveson, 2004) and also handling attacks, both physical attacks on plants (Whiteley, 2006) and cyber attacks (there are a number of results in this direction, for which a sample is Cárdenas et al. (2011), Ralston et al. (2007); on plant control systems. It is important to consider questions that are relevant to software design in the development of new control designs with system-theoretic safety constraints. Such control designs have the potential to be more complex (in terms of the number of lines of code and if/then-type statements) than standard control designs due to the added constraints, and reliable software design for such cases, and also ensuring communication between all controllers for the system if they are not fully centralized, is essential for realizing the vision developed in this tutorial of an effective integrated safety and control system design. The need to adequately test and validate software is especially important to investigate with new control designs like EMPC for which it may be difficult to know *a priori* what the process state trajectory should be and what all the possible unexpected behaviors may be, which may make validating the control software more difficult (Jaffe et al., 1991). As the control designs take a more proactive role in maintaining process operational safety and as, potentially, the safety system is equipped with more logic functionality, it will also be critical to examine how cyber security questions can be addressed to ensure that safe process operation is not interrupted in designs increasingly reliant on computer algorithms. Byres and Lowe (2004) indicates that coordination of the control and safety systems may be helpful when cyber attacks occur in control systems because then the safety system can still take actions to prevent incidents. Finally, it is notable that integrated design of the control and safety systems may be beneficial for addressing some of the issues like physical attacks on plants that are outside the scope of operational safety (which does not take into account targeted efforts by humans to disrupt the safety features of the automated elements of the system but instead focuses on operation that may be disrupted by equipment failures), which may benefit from the coordination of these automated features for trying to reduce hazards in such unexpected situations.

4. Implications of a system-theoretic approach to characterizing safety for safety system design

Because alarms at a plant are typically the first activated element of the safety system, they can be expected to be the element of the safety system that is most affected by control designs that incorporate system-theoretic safety considerations. Alarm systems today are associated with a number of issues, including nuisance (false) alarms and missed alarms (see Wang et al., 2016 for a review of the literature on alarm issues and methods for compensating for them). Nuisance alarms are alarms that sound when the process state is not in an unsafe operating region in the sense that the fact that a measured output went outside of its recommended range does not require operator actions to prevent an incident. Missed alarms are alarms that are not triggered when the state enters an unsafe operating region because the alarm triggers do not properly account for all situations that make the state unsafe (e.g., every measured output may be within its recommended range so that an alarm does not sound, but the combination of measured outputs is one that should be associated with incidents such that it sounds an alarm) (Wang et al., 2016). The number of alarms that sound at a chemical process plant each day can be over seven times the recommended number (Rothenberg, 2009; EEMUA, 2013). An important property of alarms is that they typically are not associated with an automated action, but rather with alerting the operator to issues so that the operator can take an action if he/she decides that is appropriate. Therefore, while missed alarms are clearly problematic, nuisance alarms may prevent operators from focusing on important alarms and/or decrease their confidence in the alarm system. Many of the alarm design improvement methods reviewed in Wang et al. (2016) (e.g., Noda et al., 2011; Yang et al., 2012; Alrowaie et al., 2014; Srinivasan et al., 2004) focus on how the alarm system can be improved to reduce nuisance alarms; in this tutorial, we focus on reducing nuisance alarms by designing control systems based on system-theoretic safety metrics for which the thresholds used to define constraints in the control system are below the values that the safety metric would take if the alarms sound. This will help to prevent the state, under normal operating conditions, from causing the alarms to sound, and may therefore improve operational safety by potentially reducing the number of false alarms to improve the manner in which operators respond to the alarms that do sound.

Interactions between variables have been noted to be important in defining safe operating regions and therefore alarm triggers to prevent missed alarms (e.g., Wang et al., 2016; Brooks et al., 2004). Therefore, it is reasonable to consider that another method for preventing missed alarms would be adding the Safeness Index and thresholds upon it (higher than the threshold used within the control system so that the safety system is not immediately activated when the state hits the maximum value allowed by the control system) to the alarm system so that the alarms can sound both when measured states leave their traditional ranges and also when other anomalous behavior that may occur for measured output values within the recommended ranges occurs. Another issue that may be improved by the use of the Safeness Index in the alarm system is the prevention of alarm flooding, which is defined to be many true alarms occurring at one time, more than an operator can respond to, due to the relationships between process variables at an unsafe state. By adding a threshold on the Safeness Index to the alarm system, the operator may become alerted earlier to multivariable interactions that indicate that the state is moving in an unsafe direction that may soon activate a number of alarms. This may give the operator a chance to respond to such an alarm before an alarm flood occurs and potentially prevent some cases of alarm flooding. There is also a potential that using the Safeness Index to activate elements of the safety instrumented or safety relief systems may also be beneficial because it can account for multivariable interactions and unmeasured states that can be important to process operational safety but for which the safety instrumented and safety relief systems are not typically provided information. This may overall help to prevent missed triggering of the safety system. Future research in the direction of integrating the safety and control systems will enable further improvements in operational safety.

5. Future research directions

The above sections highlight that the vision of coordinated control and safety systems for enhancing process operational safety is far from complete. Therefore, in the following subsections, we will highlight several open research topics in this area, though many more exist.

5.1. MPC designs with safety-based constraints and empirical process models

As noted above, unmeasured states may be important for evaluating whether incidents may occur for a given process condition and therefore, constraining system-theoretic safety metrics based on the process state (rather than only the measured outputs) within MPC may enhance process operational safety. To account for unmeasured states within MPC, output feedback MPC designs with system-theoretic safety constraints should be developed and analyzed for closed-loop stability and feasibility both for static and time-varying safe operating regions. For the case that first-principles process models including the unmeasured states are available, prior developments in output feedback MPC without safety-based constraints (e.g., Ellis et al., 2014b; Lao et al., 2015) may provide a useful foundation from which to develop safety-based output feedback MPC's (and may also allow safety concerns such as sensor faults to be handled). Given the prevalence of empirical models in MPC in industry, it may also be useful to investigate the implications of utilizing empirical models (Verhaegen and Dewilde, 1992; Paduart et al., 2010) within MPC (Alanqar et al., 2015a,b) with system-theoretic safety-based constraints. It may be particularly interesting to consider how an empirical model can aid in the development of a system-theoretic safety metric such as the Safeness Index in the absence of a first-principles model, and also whether empirical models can be developed with unmeasured states that have meaning from a safety perspective to allow these states to be constrained in an output feedback safety-based MPC design based on an empirical model.

5.2. Accounting for safety system activation within model predictive control design

Because MPC's utilize state predictions in the determination of appropriate control actions to apply to the process, they offer a platform for more closely coordinating the control and safety systems through the process model. Specifically, the safety system takes actions (which typically have an on/off characteristic such as bringing a valve from its fully open to fully closed position and therefore change the process dynamics and potentially the input availability in the case that, for example, the valve actuated by the safety system is in series with the valve actuated by the control system) in response to predefined triggers based on the process states. MPC's should therefore be designed that account for the activation of the safety system (e.g., they anticipate its activation at a time in the prediction horizon when the predefined triggers are exceeded) in the process model used for making state predictions to avoid significant plant-model mismatch throughout the prediction horizon that may cause the MPC to choose less suitable control actions (from both an economics viewpoint and a safety constraint viewpoint) than it would choose if it was aware of the change in the plant due to safety system activation.

Another potential means by which the control and safety systems may be coordinated (and by which the actions of the safety system may be coordinated with one another) within an MPC framework is by augmenting the traditional pre-set triggers of the safety instrumented system with an MPC-based triggering mechanism that determines appropriate actions of the safety instrumented system to maintain the state within a safe operating region when closed-loop state predictions indicate that based on the current state measurement, the available control energy is not sufficient to prevent the state from entering undesirable operating regions. This framework has the potential to enhance the ability of the safety instrumented system to act far enough in advance of an accident to prevent the accident given the nonlinear, coupled process dynamics and knowledge of how the controller will behave (a method for proactive alarm activation based on state predictions was developed in Ahooyi et al. (2016)). To develop an MPC-based framework for proactive activation of the safety instrumented system, a variety of research topics must be pursued, including the development of MPC designs for hybrid systems with general objective functions and *a priori* unknown times of safety system activation (potentially building on prior developments of MPC with general objective functions for hybrid systems such as that in Heidarinejad et al. (2013) for which the time at which the model is switched is assumed to be known) and MPC designs that are mixed-integer nonlinear programs (Bonami et al., 2008; Burer and Letchford, 2012; Boukouvala et al., 2016) (to account for the continuous nature of the control actions and the discrete nature of the actions taken by the safety instrumented systems), potentially also containing the switching models, safety-based constraints, and a general objective function, along with the characterization of theoretical properties such as closed-loop stability and recursive feasibility for the resulting designs.

5.3. System-theoretic safety metric development for distributed parameter and large-scale systems and its use in MPC

The Safeness Index reviewed in this tutorial represents only the first step in defining system-theoretic safety metrics that can be constrained in control design to enhance process operational safety, and many open research topics in this direction remain. For example, the development of a system-theoretic safety metric for distributed parameter systems should be investigated, and how it can be adequately computed on-line and constrained within MPC designs. There is a potential that states that are important indicators of operational safety for a distributed parameter system may be difficult to measure on-line, such as temperature throughout a reactor. Methods for handling this should be investigated, potentially involving state estimation or other attempts to obtain indications of the required information from readily available measurements. Techniques also must be developed for incorporating predictions of all states of the distributed parameter system that are important for evaluating safety within the MPC design in a computationally-efficient manner (e.g., the appropriateness of utilizing reduced-order models within MPC for capturing the dominant dynamics of the states that appear in the system-theoretic safety metric could be evaluated García et al., 2012; Kwon et al., 2014; Lao et al., 2014a).

Other important considerations in the development of system-theoretic safety metrics and their incorporation within MPC design are the questions of (1) whether they should include dependencies on quantities besides states (e.g., dependencies on inputs to account for actuator faults within the safety metric or dependencies on disturbances) or be formulated differently during start-up and shut-down than during normal operation, and (2) whether a single metric is sufficient for handling process safety. The latter is a concern because for large chemical plants that consist of a large number of units (leading to, potentially, hundreds or thousand of states), a single system-theoretic safety metric such as the Safeness Index may not be able to effectively capture all safety considerations at a plant. The metric may need to incorporate a large number of states across many process units so that it may be difficult to weight the terms in the metric and/or to assign an appropriate threshold on it in a manner that does not cause some unsafe values of the safety metric to fall below any reasonable threshold. To overcome this issue, multiple system-theoretic safety metrics may be constructed, such as a metric for every unit at a plant complemented by a system-theoretic metric that accounts for interactions between units that may lead to incidents. The implications of having multiple metrics in safety-based MPC designs should be considered, both for centralized and distributed designs. For the distributed designs, a methodology for partitioning the various safety metric-based constraints between the distributed controllers should be developed that can maintain closed-loop stability and can maintain the state within a safe operating region without making it difficult to achieve a feasible solution to the optimization problems (each of the distributed optimization problems has less flexibility compared to a centralized design to ensure that all of the safety metric-based constraints are satisfied with the limited control actions which it can adjust). Other control architectures (e.g., decentralized control designs Raimondo et al., 2007) may also be investigated.

5.4. Safety-based model predictive control of nonlinear systems: handling asynchronous, delayed measurements

A challenge in maintaining closed-loop stability of nonlinear systems under feedback control is that state measurements required for computing a feedback control action may be asynchronous or delayed due to measuring difficulties of some process states (e.g., species concentrations) or communication network malfunctions introducing data losses and time-varying delays. Methods for handling asynchronous and delayed measurements must be extended to MPC with safety-based constraints that guarantee closed-loop stability, and it should be investigated whether the safety metric-based constraints must be adjusted (i.e., using modified thresholds compared to those which would be utilized for synchronous measurements) to account for uncertain sampling rates. In addition, given the practicality of distributed control architectures for industrial use based on their potential computation time benefits, asynchronous and delayed measurements in the context of distributed MPC with safety metric-based constraints should be investigated, taking advantage of principles developed for distributed MPC designs with asynchronous and delayed measurements (but without safety metric-based constraints) in works such as Liu et al. (2012). A final topic that warrants attention is the practical issue of linear and nonlinear empirical models utilized in both centralized and distributed MPC with safety metric-based constraints and asynchronous/delayed measurements, and the conditions under which closed-loop stability and feasibility are guaranteed in such cases.

5.5. Ensuring operational safety of a closed-loop system with safety metric-based constraints and actuator faults

For MPC designs with system-theoretic safety metric constraints, the available actuation energy may not be sufficient for driving the process state into a safe operating region when actuator faults occur. To address safety concerns arising from actuator faults for MPC designs with safety metric-based constraints, an off-line (i.e., before process operation begins) characterization of the functional form of the safety metric when one actuator fails at a time may be investigated. Control designs with safety metric-based constraints can then be designed for which the safety metric is changed when an actuator fault occurs such that an actuator is lost. The conditions which guarantee closed-loop stability and feasibility of a nonlinear process operated under a safety metric-based MPC at the time of an actuator fault should then be investigated, potentially building on the results in Lao et al. (2014b) for MPC designs with a general objective function and actuator loss (but no safety metric-based constraints). Challenges that may need to be addressed include how to ensure process operational safety, feasibility, and closed-loop stability when a distributed control architecture is used or when multiple safety metrics are employed when an actuator is lost. Finally, because thresholds on the system-theoretic safety metrics may be determined using process data, and no data corresponding to operation with the fault condition is available until the fault occurs (Alanqar et al., 2017c), a methodology for updating the thresholds on the safety metric for both the control and safety systems on-line as data is generated after the fault must be developed.

6. Conclusion

This tutorial article reviews the developments in the literature regarding system-theoretic safety metrics and control designs containing these safety metrics with the intent of showing that though recent works based on a Safeness Index have sought to account for safety in a systems engineering context and also to allow coordination between the safety and control systems, there is significant work that must be done to enhance process operational safety through tighter coordination of those systems. We provided insights regarding the relationships of a number of works that consider safety in MPC, but without explicitly defining a system-theoretic safety metric, to MPC designs based on a Safeness Index, unifying the literature in this area and therefore showcasing the breadth of control designs that have been developed to incorporate a system-theoretic safety perspective under certain assumptions with guaranteed closed-loop stability, feasibility, and robustness properties, even for the case that the Safeness Index changes over time. Our analysis developed a list of several desirable properties for MPC's that enhance process operational safety to inspire further research in this area, and also allowed us to identify several other research directions that should be pursued to enhance process operational safety.

Acknowledgments

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

References

Abate, A., Prandini, M., Lygeros, J., Sastry, S., 2008. Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems. Automatica 44, 2724–2734.

Abel, O., Marquardt, W., 1998. A model predictive control scheme for safe and optimal operation of exothermic semi-batch reactors. In: Proceedings of the IFAC Symposium on Dynamics and Control of Process Systems, Including Biosystems, Corfu, Greece, pp. 725–730.

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.

Alanqar, A., Durand, H., Christofides, P.D., 2015a. On identification of well-conditioned nonlinear systems: application to economic model predictive control of nonlinear processes. AIChE J. 61, 3353–3373.

Alanqar, A., Ellis, M., Christofides, P.D., 2015b. Economic model predictive control of nonlinear process systems using empirical models. AIChE J. 61, 816–830.

Alanqar, A., Durand, H., Albalawi, F., Christofides, P.D., 2017a. An economic model predictive control approach to integrated production management and process operation. AIChE J. 63, 1892–1906.

Alanqar, A., Durand, H., Christofides, P.D., 2017b. Error-triggered on-line model identification for model-based feedback control. AIChE J. 63, 949–966.

Alanqar, A., Durand, H., Christofides, P.D., 2017c. Fault-tolerant economic model predictive control using error-triggered online model identification. Ind. Eng. Chem. Res. 56, 5652–5667.

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., 2017a. Achieving operational process safety via model predictive control. J. Loss Prevent. Process Ind. (in press).

Albalawi, F., Durand, H., Christofides, P.D., 2017b. Distributed economic model predictive control for operational safety of nonlinear processes. AIChE J. 63, 3404–3418.

Albalawi, F., Durand, H., Christofides, P.D., 2017c. Distributed economic model predictive control with Safeness-Index based constraints for nonlinear systems. Syst. Control Lett. 110, 21–28.

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

Alessandretti, A., Aguiar, A.P., Jones, C.N., 2016. On convergence and performance certification of a continuous-time economic model predictive control scheme with time-varying performance index. Automatica 68, 305–313.

Alrowaie, F., Gopaluni, R.B., Kwok, K.E., 2014. Alarm design for nonlinear stochastic systems. In: Proceeding of the 11th World Congress on Intelligent Control and Automation, Shenyang, China, pp. 473–479.

Amrit, R., Rawlings, J.B., Angeli, D., 2011. Economic optimization using model predictive control with a terminal cost. Annu. Rev. Control 35, 178–186.

Angeli, D., Amrit, R., Rawlings, J.B., 2012. On average performance and stability of economic model predictive control. IEEE Trans. Autom. Control 57, 1615–1626.

Aswani, A., Gonzalez, H., Sastry, S.S., Tomlin, C., 2013. Provably safe and robust learning-based model predictive control. Automatica 49, 1216–1226.

Bacci di Capaci, R., Vaccari, M., Pannocchia, G., 2017. A valve stiction tolerant formulation of MPC for industrial processes. In: Proceedings of the 20th IFAC World Congress, Toulouse, France, pp. 9374–9379.

Bakolas, E., Saleh, J.H., 2010. Augmenting the traditional defense-in-depth strategy with the concept of a diagnosable safety architecture. In: Briš, R., Soares, C.G., Martorell, S. (Eds.), Reliability, Risk and Safety: Theory and Applications, 3. CRC Press/Balkema, Leiden, Netherlands, pp. 2113–2122.

Bloch, K., 2016. Rethinking Bhopal: A Definitive Guide to Investigating, Preventing, and Learning from Industrial Disasters. Elsevier, Amsterdam, Netherlands.

Bonami, P., Biegler, L.T., Conn, A.R., Cornuéjols, G., Grossmann, I.E., Laird, C.D., Lee, J., Lodi, A., Margot, F., Sawaya, N., Wächter, A., 2008. An algorithmic framework for convex mixed integer nonlinear programs. Discrete Optim. 5, 186–204.

Boukouvala, F., Misener, R., Floudas, C.A., 2016. Global optimization advances in Mixed-Integer Nonlinear Programming, MINLP, and Constrained Derivative-Free Optimization, CDFO. Eur. J. Oper. Res. 252, 701–727.

Brooks, R., Thorpe, R., Wilson, J., 2004. A new method for defining and managing process alarms and for correcting process operation when an alarm occurs. J. Hazard. Mater. 115, 169–174.

Burer, S., Letchford, A.N., 2012. Non-convex mixed-integer nonlinear programming: a survey. Surv. Oper. Res. Manag. Sci. 17, 97–106.

Byres, E., Lowe, J., 2004. The myths and facts behind cyber security risks for industrial control systems. In: Proceedings of the VDE Kongress, Berlin, Germany.

Camacho, E.F., Bordons, C., 2007. Model Predictive Control, Second ed. Springer-Verlag, London, England.

Cárdenas, A.A., Amin, S., Lin, Z.S., Huang, Y.L., Huang, C.Y., Sastry, S., 2011. Attacks against process control systems: Risk assessment, detection, and response. In: Proceedings of the ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, pp. 355–366.

Carson III, J.M., Açıkmeşe, B., Murray, R.M., MacMartin, D.G., 2013. A robust model predictive control algorithm augmented with a reactive safety mode. Automatica 49, 1251–1260.

Center for Chemical Process Safety, 1998. Guidelines for Pressure Relief and Effluent Handling Systems. American Institute of Chemical Engineers, New York, NY.

Center for Chemical Process Safety, 2000. Guidelines for Chemical Process Quantitative Risk Analysis, Second ed. American Institute of Chemical Engineers, New York, NY.

Center for Chemical Process Safety, 2001. Layer of Protection Analysis – Simplified Process Risk Assessment. American Institute of Chemical Engineers, New York, NY.

Center for Chemical Process Safety, 2008. Guidelines for Hazard Evaluation Procedures, Third ed. John Wiley & Sons, Inc., Hoboken, NJ.

Center for Chemical Process Safety, 2010. Guidelines for Process Safety Metrics. John Wiley & Sons, Inc., Hoboken, NJ.

Center for Chemical Process Safety, 2017a. Appendix D. Alarm management. In: Guidelines for Safe Automation of Chemical Processes, Second ed. John Wiley & Sons, Inc., Hoboken, NJ, pp. 423–439.

Center for Chemical Process Safety, 2017b. Guidelines for Safe Automation of Chemical Processes, Second ed. John Wiley & Sons, Inc., 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.

Cowlagi, R.V., Saleh, J.H., 2015. Coordinability and consistency: application of systems theory to accident causation and prevention. J. Loss Prevent. Process Ind. 33, 200–212.

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

Diehl, M., Amrit, R., Rawlings, J.B., 2011. A Lyapunov function for economic optimizing model predictive control. IEEE Trans. Autom. Control 56, 703–707.

Durand, H., Christofides, P.D., 2016. Actuator stiction compensation via model predictive control for nonlinear processes. AIChE J. 62, 2004–2023.

Durand, H., Ellis, M., Christofides, P.D., 2016. Economic model predictive control designs for input rate-of-change constraint handling and guaranteed economic performance. Comput. Chem. Eng. 92, 18–36.

EEMUA, 2013. EEMUA-191: Alarm Systems - A Guide to Design, Management and Procurement. Engineering Equipment and Materials Users Association, London, England.

Ellis, M., Durand, H., Christofides, P.D., 2014a. A tutorial review of economic model predictive control methods. J. Process Control 24, 1156–1178.

Ellis, M., Zhang, J., Liu, J., Christofides, P.D., 2014b. Robust moving horizon estimation based output feedback economic model predictive control. Syst. Control Lett. 68, 101–109.

Ellis, M., Durand, H., Christofides, P.D., 2016. Elucidation of the role of constraints in economic model predictive control. Annu. Rev. Control 41, 208–217.

Englund, S.M., 2007. Safety considerations in the chemical process industries. In: Kent, J.A. (Ed.), Kent and Riegel's Handbook of Industrial Chemistry and Biotechnology. , Eleventh ed. Springer, New York, NY, pp. 83–146.

Fisher, H.G., Forrest, H.S., Grossel, S.S., Huff, J.E., Muller, A.R., Noronha, J.A., Shaw, D.A., Tilley, B.J., 1992. Emergency Relief System Design Using DIERS Technology – The Design Institute for Emergency Relief Systems (DIERS) Project Manual. American Institute for Chemical Engineers, New York, NY.

García, M.R., Vilas, C., Santos, L.O., Alonso, A.A., 2012. A robust multi-model predictive controller for distributed parameter systems. J. Process Control 22, 60–71.

Gillula, J.H., Huang, H., Vitus, M.P., Tomlin, C.J., 2010. Design of guaranteed safe maneuvers using reachable sets: autonomous quadrotor aerobatics in theory and practice. In: Proceedings of the IEEE International Conference on Robotics and Automation, Anchorage, Alaska, pp. 1649–1654.

Heidarinejad, M., Liu, J., Christofides, P.D., 2012. Economic model predictive control of nonlinear process systems using Lyapunov techniques. AIChE J. 58, 855–870.
Heidarinejad, M., Liu, J., Christofides, P.D., 2013. Economic model predictive control of switched nonlinear systems. Syst. Control Lett. 62, 77–84.
Huang, R., Biegler, L.T., Harinath, E., 2012. Robust stability of economically oriented infinite horizon NMPC that include cyclic processes. J. Process Control 22, 51–59.
Jaffe, M.S., Leveson, N.G., Heimdahl, M.P.E., Melhart, B.E., 1991. Software requirements analysis for real-time process-control systems. IEEE Trans. Softw. Eng. 17, 241–258.
Jones, S., Kirchsteiger, C., Bjerke, W., 1999. The importance of near miss reporting to further improve safety performance. J. Loss Prevent. Process Ind. 12, 59–67.
Kazantzis, N., Kravaris, C., 1998. Nonlinear observer design using Lyapunov's auxiliary theorem. Syst. Control Lett. 34, 241–247.
Kettunen, M., Zhang, P., Jämsä-Jounela, S.L., 2008. An embedded fault detection, isolation and accommodation system in a model predictive controller for an industrial benchmark process. Comput. Chem. Eng. 32, 2966–2985.
Khalil, H.K., 2002. Nonlinear Systems, Third ed. Prentice Hall, Upper Saddle River, NJ.
Khalil, H.K., Esfandiari, F., 1993. Semiglobal stabilization of a class of nonlinear systems using output feedback. IEEE Trans. Autom. Control 38, 1412–1415, 10.1109/9.237658.
Khan, F.I., Amyotte, P.R., 2003. How to make inherent safety practice a reality. Can. J. Chem. Eng. 81, 2–16.
Kidam, K., Hurme, M., 2013. Analysis of equipment failures as contributors to chemical process accidents. Process Saf. Environ. Protect. 91, 61–78.
Kim, K.D., Kumar, P.R., 2014. An MPC-based approach to provable system-wide safety and liveness of autonomous ground traffic. IEEE Trans. Autom. Control 59, 3341–3356.
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.
Kwon, J.S.I., Nayhouse, M., Orkoulas, G., Christofides, P.D., 2014. Enhancing the crystal production rate and reducing polydispersity in continuous protein crystallization. Ind. Eng. Chem. Res. 53, 15538–15548.
Lao, L., Ellis, M., Christofides, P.D., 2013. Proactive fault-tolerant model predictive control. AIChE J. 59, 2810–2820.
Lao, L., Ellis, M., Christofides, P.D., 2014a. Economic model predictive control of transport-reaction processes. Ind. Eng. Chem. Res. 53, 7382–7396.
Lao, L., Ellis, M., Christofides, P.D., 2014b. Smart Manufacturing: handling preventive actuator maintenance and economics using model predictive control. AIChE J. 60, 2179–2196.
Lao, L., Ellis, M., Durand, H., Christofides, P.D., 2015. Real-time preventive sensor maintenance using robust moving horizon estimation and economic model predictive control. AIChE J. 61, 3374–3389.
Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42, 237–270.
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.
Liu, J., Chen, X., Muñoz de la Peña, D., Christofides, P.D., 2012. Iterative distributed model predictive control of nonlinear systems: handling asynchronous, delayed measurements. IEEE Trans. Autom. Control 57, 528–534.
Mũnoz 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.
Mannan, S., 2012. Lees' Loss Prevention in the Process Industries – Hazard Identification, Assessment and Control, Fourth ed. Elsevier, Waltham, MA.
Marlin, T., 2012. Operability in Process Design: Achieving Safe, Profitable, and Robust Process Operations. McMaster University, Ontario, Canada.
Marlin, T.E., Hrymak, A.N., 1996. Real-time operations optimization of continuous processes. In: Proceedings of the Fifth International Conference on Chemical Process Control, Tahoe City, CA, pp. 156–164.
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.
Meel, A., Seider, W.D., 2006. Plant-specific dynamic failure assessment using Bayesian theory. Chem. Eng. Sci. 61, 7036–7056.
Mhaskar, P., 2006. Robust model predictive control design for fault-tolerant control of process systems. Ind. Eng. Chem. Res. 45, 8565–8574.
Mhaskar, P., El-Farra, N.H., Christofides, P.D., 2006. Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. Syst. Control Lett. 55, 650–659.
Mhaskar, P., Kennedy, A.B., 2008. Robust model predictive control of nonlinear process systems: handling rate constraints. Chem. Eng. Sci. 63, 366–375.
Morari, M., Lee, J.H., 1999. Model predictive control: past, present and future. Comput. Chem. Eng. 23, 667–682.
Müller, M.A., Allgöwer, F., 2017. Economic and distributed model predictive control: recent developments in optimization-based control. SICE J. Control Meas. Syst. Integr. 10, 39–52.
Ness, A., 2015. Lessons learned from recent process safety incidents. Chem. Eng. Prog., 23–29.
Noda, M., Higuchi, F., Takai, T., Nishitani, H., 2011. Event correlation analysis for alarm system rationalization. Asia-Pac. J. Chem. Eng. 6, 497–502.
de Oliveira Kothare, S.L., Morari, M., 2000. Contractive model predictive control for constrained nonlinear systems. IEEE Trans. Autom. Control 45, 1053–1071.
Paduart, J., Lauwers, L., Swevers, J., Smolders, K., Schoukens, J., Pintelon, R., 2010. Identification of nonlinear systems using Polynomial Nonlinear State Space models. Automatica 46, 647–656.
Pantoleontos, G., Kikkinides, E.S., Georgiadis, M.C., 2012. A heterogeneous dynamic model for the simulation and optimisation of the steam methane reforming reactor. Int. J. Hydrogen Energy 37, 16346–16358.
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. Industrial & Engineering Chemistry Research 49, 8062–8079.
Phimister, J.R., Oktem, U., Kleindorfer, P.R., Kunreuther, H., 2003. Near-miss incident management in the chemical process industry. Risk Anal. 23, 445–459.
Piché, S., Sayyar-Rodsari, B., Johnson, D., Gerules, M., 2000. Nonlinear model predictive control using neural networks. IEEE Control Syst. Mag., 53–62.
Prakash, J., Patwardhan, S.C., Narasimhan, S., 2002. A supervisory approach to fault-tolerant control of linear multivariable systems. Ind. Eng. Chem. Res. 41, 2270–2281.
Qin, S.J., Badgwell, T.A., 2003. A survey of industrial model predictive control technology. Control Eng. Pract. 11, 733–764.
Raimondo, D.M., Magni, L., Scattolini, R., 2007. Decentralized MPC of nonlinear systems: an input-to-state stability approach. Int. J. Robust Nonlinear Control 17, 1651–1667.
Ralston, P.A.S., Graham, J.H., Hieb, J.L., 2007. Cyber security risk assessment for SCADA and DCS networks. ISA Trans. 46, 583–594.
Rawlings, J.B., Angeli, D., Bates, C.N., 2012. Fundamentals of economic model predictive control. In: Proceedings of the 51st IEEE Conference on Decision and Control, Maui, Hawaii, pp. 3851–3861.
Reniers, G., Cozzani, V. (Eds.), 2013. Domino Effects in the Process Industries: Modeling, Prevention and Managing. Elsevier, Waltham, MA.
Rothenberg, D.H., 2009. Alarm Management for Process Control: A Best-Practice Guide for Design, Implementation, and Use of Industrial Alarm Systems. Momentum Press, New York, NY.
Srinivasan, R., Liu, J., Lim, K.W., Tan, K.C., Ho, W.K., 2004. Intelligent alarm management in a petroleum refinery. Hydrocarbon Process. 83, 47–53.
Srinivasan, R., Rengaswamy, R., 2008. Approaches for efficient stiction compensation in process control valves. Comput. Chem. Eng. 32, 218–229.
Venkatasubramanian, V., 2011. Systemic failures: challenges and opportunities in risk management in complex systems. AIChE J. 57, 2–9.
Venkatasubramanian, V., Zhao, J., Viswanathan, S., 2000. Intelligent systems for HAZOP analysis of complex process plants. Comput. Chem. Eng. 24, 2291–2302.
Verhaegen, M., Dewilde, P., 1992. Subspace model identification part 1. The output-error state-space model identification class of algorithms. Int. J. Control 56, 1187–1210.
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.
Whiteley, J.R., 2006. Potential use of advanced process control for safety purposes during attack of a process plant. J. Hazard. Mater. 130, 42–47.
Wieber, P.B., 2008. Viability and predictive control for safe locomotion. In: Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems, Nice, France, pp. 1103–1108.
Wu, Z., Aguirre, A., Tran, A., Durand, H., Ni, D., Christofides, P.D., 2017. Model predictive control of a steam methane reforming reactor described by a computational fluid dynamics model. Ind. Eng. Chem. Res. 56, 6002–6011.
Yang, F., Shah, S.L., Xiao, D., Chen, T., 2012. Improved correlation analysis and visualization of industrial alarm data. ISA Trans. 51, 499–506.