Operational Safety of Chemical Processes via Safe Model Predictive Control

Fahad Albalawi[1], Helen Durand[2] and Panagiotis D. Christofides[*,1,2]

[1]Department of Electrical Engineering, University of California, Los Angeles, CA 90095-1592
[2]Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592

Abstract

This paper highlights our recent work on the integration of operational safety considerations with process control via Lyapunov-based model predictive control to form a framework termed safety-LMPC. Specifically, we review the formulation of the safety-LMPC optimization problem, including the time-varying safety-based constraints that guarantee closed-loop stability and recursive feasibility. When the objective function of the safety-LMPC takes a standard tracking form, the safety-based constraints can enhance the rate at which the closed-loop state approaches the steady-state. When an economics-based objective function is used (safety-LEMPC), the resulting controller can drive the process state between various safe regions of operation and maintain the state there while continuously optimizing process economics. Because it is possible that significant computation delay may result when computing control actions for large-scale nonlinear processes, a distributed model predictive controller with safety-based constraints can be used to improve the computation time with respect to the centralized safety-LMPC.

Keywords

Process safety, safe operating regions, process economics, model predictive control, nonlinear processes.

Introduction

Process safety is critical in the chemical and petrochemical industries. In these industries, two important methods for protecting against unsafe scenarios are improving process inherent safety (i.e., the innate safeness of the process based on its chemistry and physics) and designing effective control systems (Crowl and Louvar (2011)). Leveson and Stephanopoulos (2014) have argued that process safety and feedback control can be combined in one framework. However, the traditional single-input/single-output feedback control loop lacks many of the capabilities that a process control system should have to ensure process safety such as the ability to account for process input and state constraints.

In the last several decades, modern control techniques have been developed that can enhance process safety. For instance, tracking model predictive control (MPC), which is widely adopted in industry, is a control strategy that dictates driving and keeping the process state at the optimal steady-state while taking restrictions on process inputs and states into account (e.g., Leveson and Stephanopoulos (2014); Qin and Badgwell (2003)). Several research works have consequently focused on incorporating safety considerations within model predictive control (Carson et al. (2013)). Over the past decades, a form of MPC termed Lyapunov-based MPC (LMPC) (Mhaskar et al. (2006)) has gained attention because of its guaranteed closed-loop stability properties. However, the rate at which the LMPC drives the closed-loop state toward the equilibrium using the quadratic objective function and Lyapunov-based constraints alone may not be fast enough to ensure process safety or this rate may not be readily quantitatively-determined through the penalty terms on the cost function.

Another form of MPC termed economic model predictive control (EMPC), which dictates time-varying op-

*To whom all correspondence should be addressed, Email: *pdc@seas.ucla.edu*.

eration to integrate process economics with process control, provides a unique framework for integrating operational safety considerations and feedback control because it uses a general cost function in its formulation which can be formulated to incorporate both safety and economics considerations for the process (Angeli et al. (2012); Ellis et al. (2014)). Motivated by this, our recent work (Albalawi et al. (2016)) has developed Lyapunov-based EMPC (LEMPC) schemes with safety-based constraints termed safety-LEMPC that guarantee safe operation of a class of nonlinear process systems by varying the allowable region of operation. Both safety-LMPC and safety-LEMPC can be implemented with a distributed model predictive control (DMPC) architecture to improve the real-time computation time of the MPC algorithm (Christofides et al. (2011); Scattolini (2009)). In this work, we will outline our recent results on the integration of safety-based constraints into LMPC and LEMPC.

Class of Nonlinear Process Systems

We consider nonlinear process systems with the following state-space description:

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

where $x \in R^n$ is the state of the system, and $u \in R^m$ and $w \in R^w$ are the control (manipulated) input vector and the disturbance vector, respectively. The admissible input values are restricted to be in m nonempty convex sets $U_i \subseteq R$, $i = 1, \ldots, m$. We assume that f is a locally Lipschitz vector function of its arguments with $f(0, 0, 0) = 0$. We further assume w is bounded within the set $W := \{w \in R^w : |w| \leq \theta, \theta > 0\}$. We also constrain the class of nonlinear systems of Eq. 1 to a class of stabilizable nonlinear systems. Specifically, we assume the existence of a sufficiently smooth Lyapunov function $V(x)$ and a Lyapunov-based controller $h(x) = [h_1(x) \ \cdots \ h_m(x)]^T$ such that the nominal ($w(t) \equiv 0$) closed-loop system of Eq. 1 for $u = h(x)$ is asymptotically stable ($\dot{V}$ is negative definite in a region around the origin). The largest level set of V where $\dot{V}$ is negative is termed the stability region Ω_ρ.

Implementation Strategy of Safety-Based MPC

In industry, safety is typically implemented through a hierarchy of independent layers. The lowest layer (i.e., the first line of defense before higher layers are activated) of the safety hierarchy is process control, which contributes to safety by controlling key variables like pressure, temperature and ratios of flows to combustion processes (e.g., Marlin (2012)). Though effective process control can prevent many unsafe situations, it may not prevent hazards if very large disturbances occur or if there are deficiencies in the final control elements (e.g., valve stiction) or sensor faults. For this reason, additional safety layers such as alarms and pressure relief valves are also added to chemical process systems that activate when unsafe situations are detected that cannot be mitigated by the process control system.

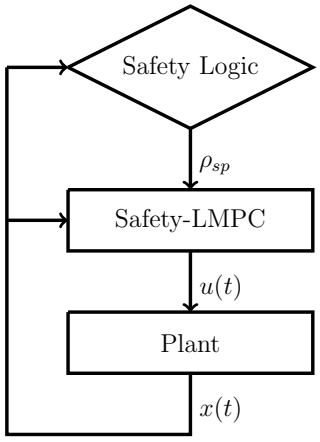

Figure 1. The implementation strategy of the safety-LMPC paradigm

Though the traditional process control techniques that are most widely adopted in the safety hierarchy such as proportional-integral-derivative (PID) control loops have successfully prevented many hazards, they cannot take multi-variable interactions between the process components or closed-loop dynamic responses into account, especially for nonlinear processes. This deficiency in their capabilities can lead to unneeded triggering of safety alarms or process shut-down. Therefore, integrating safety considerations within a control design that accounts for multi-variable interactions and closed-loop process dynamics, such as MPC, can allow the control system to take proactive actions to prevent the consequences of abnormal process conditions, providing greater robustness to the safety hierarchy in the process control layer and possibly decreasing the frequency with which higher levels of the safety hierarchy are triggered. It may also be able to account for some of the issues with sensors and final control elements that PID-type control loops are incapable of handling because it incorporates a process model and has flexibility in the formulation of the constraints. Thus, we propose that the traditional control techniques in the lowest level

of the safety hierarchy be replaced with a safety-based MPC formulation (the additional layers of the safety hierarchy continue to act independently of the process control layer).

Because safety considerations often take the form of bounds on process variables, an ideal MPC formulation for incorporating safety-based considerations is Lyapunov-based model predictive control (LMPC) because it is a model-based control framework that enforces process operation within a specific region of state-space (the stability region). The safety-based constraints are developed to maintain the closed-loop state within a safe region of operation or to move it to a region determined by a data processing unit (safety logic unit) to be more safe. This implementation strategy for safety-LMPC is shown in Figure 1. After determining the safest Lyapunov level set $\Omega_{\rho_{sp}}$ (safety region/safety level set) for the process to operate within based on data such as the likelihood of an equipment or software failure or other unsafe scenario, the safety logic unit communicates the safety set-point ρ_{sp} to the safety-LMPC. Subsequently, the safety-LMPC computes control actions that drive the closed-loop state into $\Omega_{\rho_{sp}}$ and maintain process operation there. After the safety-LMPC applies the control actions to the plant in a sample-and-hold fashion, the measured process state will be fed back to both the safety-LMPC for controller robustness and the safety logic unit so that the safety level set will be re-evaluated if necessary. One important point to be made is that the safety level sets into which the safety-LMPC drives the closed-loop state account for the ability of the control system, subject to the input constraints, to control the process state there. The mathematical formulation of the safety-based constraints that achieve these goals will be discussed in the following sections.

Incorporation of Safety-Based Constraints Within Tracking MPC

In this section, we present the formulation of safety-based constraints for LMPC with a tracking (quadratic) objective function for consistency with the tracking MPC formulation commonly used in the chemical process industries (Albalawi et al. (2017a)). The motivation for using safety-based constraints in this context is that these constraints may cause the rate at which the closed-loop state moves toward the origin when safety concerns arise to be faster than it would be under the standard LMPC without safety-based constraints. The rate of approach to the steady-state under the standard LMPC is no slower than the worst-case rate at which $h(x)$ would drive the system to the steady-state when implemented in sample-and-hold, but otherwise is determined by the weighting matrices Q and R and the penalties they place on deviations of the states and inputs from their steady-state values. This LMPC formulation offers no flexibility to change the rate of approach to the steady-state when the safety logic unit determines that the state needs to move to a smaller region of operation quickly to avoid safety alarms or process shut-down. The proposed safety-LMPC overcomes these disadvantages and is formulated as follows:

$$\min_{u(t),K_c(t)\in S(\Delta)} \int_{t_k}^{t_{k+N}} [\tilde{x}(\tau)^T Q\tilde{x}(\tau) + u(\tau)^T Ru(\tau) + \phi(\rho_{sp} - \tilde{\rho}(\tau))d\tau] \quad (2a)$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \quad (2b)$$

$$u(t) \in U, \ \forall \ t \in [t_k, t_{k+N}) \quad (2c)$$

$$\tilde{x}(t_k) = x(t_k) \quad (2d)$$

$$K_c(t) \geq 0, \ \forall \ t \in [t_k, t_{k+N}) \quad (2e)$$

$$V(\tilde{x}(t)) \leq \tilde{\rho}(t), \ \forall \ t \in [t_k, t_{k+N}) \quad (2f)$$

$$\frac{d\tilde{\rho}}{dt} = K_c(t)(\rho_{sp} - \tilde{\rho}(t)) \quad (2g)$$

$$\tilde{\rho}(t_k) = V(x(t_k)), \quad \text{if } x(t_k) \notin \Omega_{\rho_{sp}}$$
$$\tilde{\rho}(t_k) = \rho_{sp}, \quad \text{if } x(t_k) \in \Omega_{\rho_{sp}} \quad (2h)$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0) \quad (2i)$$

where $S(\Delta)$ is the set of piecewise-constant vector functions with period Δ. The optimization variables are the piecewise-constant input trajectory $u(t)$ over the prediction horizon with N sampling periods of length Δ, as well as the piecewise-constant auxiliary variable $K_c(t)$ that plays a role in the safety-based constraints. This safety-LMPC formulation contains many of the standard constraints utilized in MPC (e.g., a nominal process model for the predicted state $\tilde{x}$ (Eq. 2b), input constraints (Eq. 2c), state feedback (Eq. 2d), and quadratic terms containing Q and R in the objective function (Eq. 2a)), but also includes a safety penalty function $\phi(\cdot)$ in the objective function, as well as safety-based constraints (Eqs. 2e-2h) and a contractive constraint (Eq. 2i). The contractive constraint (Eq. 2i) ensures that the Lyapunov function value always decreases between two sampling periods (i.e., the closed-loop state

always moves toward the origin) until the closed-loop state enters a neighborhood of the origin, but the safety-based constraints of Eqs. 2e-2h are used to speed the rate at which the closed-loop state approaches the safety region when possible. They achieve this due to the penalty in the objective function on the deviation of the predicted upper bound of the Lyapunov function ($\tilde{\rho}(t)$) from ρ_{sp}. This penalty causes the safety-LMPC to seek to decrease $\tilde{\rho}(t)$. Specifically, $\tilde{\rho}(t)$ is decreased by Eq. 2g if a positive value of $K_c(t)$ is found for which an input $u(t)$ can be found to decrease $\tilde{x}(t)$ at a rate that allows Eq. 2f to be satisfied at all times for the rate of decrease of $\tilde{\rho}$ from Eq. 2g. The dynamic constraint of Eq. 2g allows $\tilde{\rho}$ to be decreased throughout the prediction horizon, and with a significant penalty on $(\rho_{sp} - \tilde{\rho}(t))$ in the objective function, the LMPC will compute values of $u(t)$ and $K_c(t)$ that decrease $\tilde{\rho}(t)$ quickly, and thus, move the predicted state toward $\Omega_{\rho_{sp}}$ quickly through Eq. 2f. When the closed-loop state is predicted to move toward $\Omega_{\rho_{sp}}$ quickly, the actual closed-loop state may also move toward $\Omega_{\rho_{sp}}$ more quickly than if the safety-based constraints were not utilized. Once the closed-loop state enters $\Omega_{\rho_{sp}}$, the value of $\tilde{\rho}$ becomes fixed at ρ_{sp}, and the safety-LMPC of Eq. 2 becomes the standard LMPC design. Thus, process safety is enhanced by this design because it allows different regions of safe operation to be determined on-line and allows the controller to respond to such changes in a way that brings the closed-loop state into a safe region of operation at a possibly faster rate than if the safety-based constraints were not incorporated. In addition, the safety-LMPC formulation, with a slight adjustment to the regions that trigger the use of the different initial values of $\tilde{\rho}$ in Eq. 2h, can be proven to drive the closed-loop state into $\Omega_{\rho_{sp}}$ and to maintain it there (i.e., rigorous closed-loop stability and feasibility properties exist).

Incorporation of Safety-Based Constraints Within EMPC

When the stage cost used with safety-LMPC is an economics-based objective function (to form safety-LEMPC), two modifications can be made to the safety-LMPC design of Eq. 2 so that the resulting safety-LEMPC design promotes time-varying operation within a safe region of operation (Albalawi et al. (2016)). The two modifications are that the quadratic term in the objective function is replaced by a general stage cost $L_e(\tilde{x}(\tau), u(\tau))$ that reflects the process economics so that the following objective function is minimized:

$$\int_{t_k}^{t_{k+N}} [L_e(\tilde{x}(\tau), u(\tau)) + \phi(\rho_{sp} - \tilde{\rho}(\tau))] d\tau \tag{3}$$

Furthermore, to allow time-varying operation within $\Omega_{\rho_{sp}}$ rather than driving the process state to the steady-state, the repeatedly enforced contractive constraint of Eq. 2i is replaced by a contractive constraint only activated when the closed-loop state is outside of $\Omega_{\rho_{sp}}$:

$$\begin{aligned} &\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \\ &\qquad \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0), \\ &\qquad \text{if } x(t_k) \in \Omega_\rho / \Omega_{\rho_{sp}} \end{aligned} \tag{4}$$

As for the safety-LMPC, the role of the safety-based constraints of Eqs. 2e-2h in the safety-LEMPC is to shrink the region of operation until the closed-loop state enters the safety region $\Omega_{\rho_{sp}}$ at a possibly faster rate than that which would be achieved without such constraints. Rigorous closed-loop stability and feasibility properties of safety-LEMPC have been investigated in Albalawi et al. (2016).

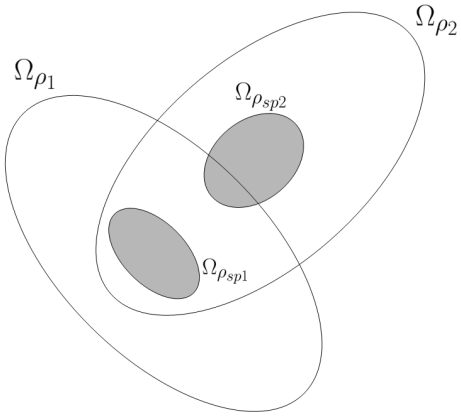

Figure 2. Configuration 1 for switching between two different safe regions of operation

Safety Region Changes

The safety-LMPC and safety-LEMPC formulations of Eqs. 2-4 assume that $\Omega_{\rho_{sp}}$ is a subset of Ω_ρ. However, there maybe scenarios in which the safety logic unit indicates that regions within the current stability region Ω_ρ are no longer safe to operate within, but that another safety region that is a subset of a different stability region is appropriate. Therefore, it is necessary to modify the safety-LMPC or safety-LEMPC formulations in a manner that allows the region of operation

to shift. The manner in which the safety-based MPC formulation should be modified depends on the configuration of the old stability and safety regions ($\Omega_{\rho 1}$ and $\Omega_{\rho_{sp1}}$ respectively) with respect to the newly requested stability and safety regions ($\Omega_{\rho 2}$ and $\Omega_{\rho_{sp2}}$ respectively). This will be illustrated by presenting two example configurations in the context of the safety-LMPC of Eq. 2, but it can be readily generalized to safety-LEMPC.

Figure 2 shows one possible configuration (Configuration 1) of the two different safe regions of operation $\Omega_{\rho_{sp1}}$ and $\Omega_{\rho_{sp2}}$. For this configuration, the safety-LMPC of Eq. 2 will be applied with $\rho_{sp} = \rho_{sp1}$ until the closed-loop state enters $\Omega_{\rho_{sp1}}$. At the switching time t_s, the safety logic unit determines that $\Omega_{\rho_{sp2}}$ is the new safe region of operation, which is a subset of the stability region $\Omega_{\rho 2}$. Therefore, at this time ρ_{sp} in the formulation of Eq. 2 will be changed to ρ_{sp2}. Because the first safety region $\Omega_{\rho_{sp1}}$ is contained within the stability region $\Omega_{\rho 2}$ and the safety-LMPC of Eq. 2 with $\rho_{sp} = \rho_{sp2}$ drives the closed-loop state into $\Omega_{\rho_{sp2}}$ from any initial condition in $\Omega_{\rho 2}$, the safety-LMPC of Eq. 2 is feasible after t_s and guarantees that the closed-loop state will be driven from $\Omega_{\rho_{sp1}}$ into $\Omega_{\rho_{sp2}}$ in finite time.

Figure 3 shows a second possible configuration (Configuration 2) of $\Omega_{\rho 1}$, $\Omega_{\rho_{sp1}}$, $\Omega_{\rho 2}$, and $\Omega_{\rho_{sp2}}$. In this case, $\Omega_{\rho_{sp1}}$ is not fully within the stability region $\Omega_{\rho 2}$. To drive the closed-loop state from any initial condition within $\Omega_{\rho_{sp1}}$ into $\Omega_{\rho_{sp2}}$ after t_s, one method is to remove the contractive constraint from Eq. 2 (formulated with $\rho_{sp} = \rho_{sp1}$) at t_s, and to replace it with a terminal region constraint (e.g., $\tilde{x}(t_{s+N}) \in \Omega_{\rho_2}$) with a sufficiently long prediction horizon to drive the closed-loop state into $\Omega_{\rho 2}$ by the end of the prediction horizon. However, due to the hard terminal constraint, feasibility of this optimization problem is not guaranteed. An alternative method for attempting the safety region transition is to remove the contractive constraint from Eq. 2 at t_s and to add a soft constraint (e.g., a penalty on $(V(\tilde{x}(t)) - \rho_2)$) in the objective function to encourage the LMPC to compute control actions that drive the closed-loop state into $\Omega_{\rho 2}$. Though this approach would always be feasible, there is still no guarantee that the state will be driven into $\Omega_{\rho 2}$. However, once the state enters $\Omega_{\rho 2}$, the LMPC problem of Eq. 2 with $\rho_{sp} = \rho_{sp2}$ could be used to drive the state into $\Omega_{\rho_{sp2}}$. These two example configurations show that the manner in which $\Omega_{\rho 1}$, $\Omega_{\rho_{sp1}}$, $\Omega_{\rho 2}$, and $\Omega_{\rho_{sp2}}$ are related to each other (e.g., how they intersect) determines how the safety-LMPC of Eq. 2 should be modified at t_s to drive the state into the new stability region, and also whether this can be achieved while guaranteeing closed-loop stability and feasibility.

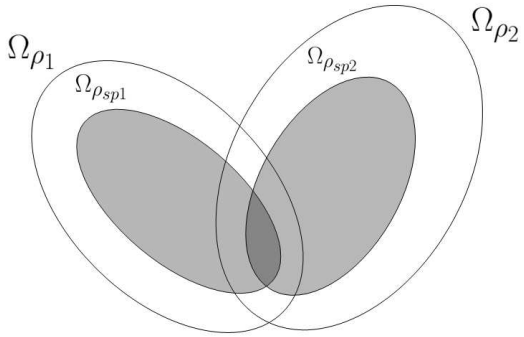

Figure 3. Configuration 2 for switching between two different safe regions of operation

Distributed Lyapunov-Based Model Predictive Control with Safety-Based Constraints

The controller designs described in the prior sections were developed with a centralized MPC structure. Thus, significant computation delay may result when computing control actions for large-scale process systems, which may affect closed-loop stability and process safety. An alternative MPC architecture that is intended to improve the computation time of the MPC algorithm is a distributed MPC (DMPC) architecture. This MPC architecture has been investigated for computation time benefits since it can reduce the number of decision variables in each of the distributed optimization problems and may be able to terminate the optimization problems before the optimal solution is found while maintaining feasibility and process closed-loop stability (Anderson et al. (2015)).

Both LMPC and LEMPC formulated with safety-based constraints can be integrated with a distributed MPC architecture. An iterative or sequential distributed control architecture can be used, and the inputs may be partitioned between the various optimization problems in the distributed structure based on their impact on process safety. The implementation strategy of an example distributed LMPC scheme is shown in Figure 4 for a safety-LEMPC scheme with a sequential distributed architecture (safety-S-DLEMPC (Albalawi et al. (2017b))). The sequential architecture in this figure consists of two controllers: Safety-S-DLEMPC 1 and Safety-S-DLEMPC 2. The formulation of Safety-S-DLEMPC 1 is that of the standard safety-LEMPC design (Eqs. 3, 2b-2h, and 4) except that only j in-

puts (i.e., $u_1(\tau|t_k), ..., u_j(\tau|t_k)$) and the gain $K_c(\tau|t_k)$, $\tau \in [t_k, t_{k+N})$, are computed by this controller, with the remaining inputs set to the values they would take using the sample-and-hold Lyapunov-based controller $h(x)$ used in the design of the stability and safety-based constraints of Safety-S-DLEMPC 1. If the inputs calculated by Safety-S-DLEMPC 1 are believed to be those with the largest impact on safety such that significant additional optimization with respect to safety is not expected within Safety-S-DLEMPC 2, the formulation of Safety-S-DLEMPC 2 can be simplified to that of the safety-LEMPC with $K_c \equiv 0$, and it can be used to improve the process economics by determining optimal values for $u_{j+1}(\tau|t_k), ..., u_m(\tau|t_k))$ after receiving from Safety-S-DLEMPC 1 the values $u_1(\tau|t_k), ..., u_j(\tau|t_k)$.

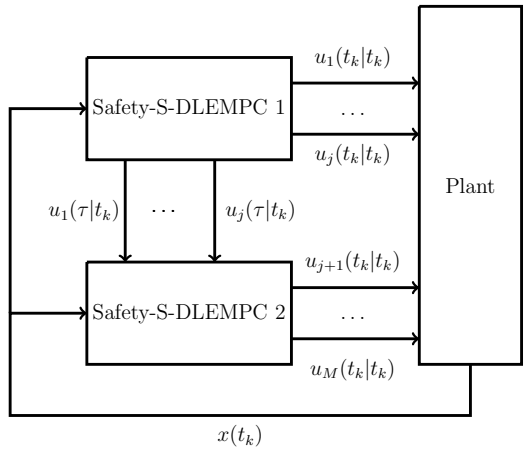

Figure 4. A block diagram of the sequential safety-DLEMPC scheme

Acknowledgments

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

References

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

Albalawi, F., Durand, H., Alanqar, A., and Christofides, P. D. (2017a). Achieving operational process safety via model predictive control. *Journal of Loss Prevention in the Process Industries*, in press.

Albalawi, F., Durand, H., and Christofides, P. D. (2017b). Distributed economic MPC with safety-based constraints for nonlinear systems. In *Proceedings of the 20th IFAC World Congress*, submitted, Toulouse, France.

Anderson, T. L., Ellis, M., and Christofides, P. D. (2015). Distributed economic model predictive control of a catalytic reactor: Evaluation of sequential and iterative architectures. In *Proceedings of the IFAC International Symposium on Advanced Control of Chemical Processes*, pages 26–31, Whistler, Canada.

Angeli, D., Amrit, R., and Rawlings, J. B. (2012). On average performance and stability of economic model predictive control. *IEEE Transactions on Automatic Control*, 57:1615–1626.

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

Christofides, P. D., Liu, J., and Muñoz de la Peña, D. (2011). *Networked and Distributed Predictive Control: Methods and Nonlinear Process Network Applications*. Springer-Verlag, London, England.

Crowl, D. A. and Louvar, J. F. (2011). *Chemical Process Safety: Fundamentals with Applications*. Pearson Education, Upper Saddle River, NJ, third edition.

Ellis, M., Durand, H., and Christofides, P. D. (2014). A tutorial review of economic model predictive control methods. *Journal of Process Control*, 24:1156–1178.

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

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

Mhaskar, P., El-Farra, N. H., and Christofides, P. D. (2006). Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. *Systems & Control Letters*, 55:650–659.

Qin, S. J. and Badgwell, T. A. (2003). A survey of industrial model predictive control technology. *Control Engineering Practice*, 11:733–764.

Scattolini, R. (2009). Architectures for distributed and hierarchical model predictive control–a review. *Journal of Process Control*, 19:723–731.