Proactive Fault-Tolerant Model Predictive Control

Liangfeng Lao and Matthew Ellis
Dept. of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095

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

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

DOI 10.1002/aic.14074
Published online March 13, 2013 in Wiley Online Library (wileyonlinelibrary.com)

Fault-tolerant control methods have been extensively researched over the last 10 years in the context of chemical process control applications, and provide a natural framework for integrating process monitoring and control aspects in a way that not only fault detection and isolation but also control system reconfiguration is achieved in the event of a process or actuator fault. But almost all the efforts are focused on the reactive fault-tolerant control. As another way for fault-tolerant control, proactive fault-tolerant control has been a popular topic in the communication systems and aerospace control systems communities for the last 10 years. At this point, no work has been done on proactive fault-tolerant control within the context of chemical process control. Motivated by this, a proactive fault-tolerant Lyapunov-based model predictive controller (LMPC) that can effectively deal with an incipient control actuator fault is proposed. This approach to proactive fault-tolerant control combines the unique stability and robustness properties of LMPC as well as explicitly accounting for incipient control actuator faults in the formulation of the MPC. Our theoretical results are applied to a chemical process example, and different scenaria were simulated to demonstrate that the proposed proactive fault-tolerant model predictive control method can achieve practical stability and efficiently deal with a control actuator fault. © 2013 American Institute of Chemical Engineers *AIChE J*, 59: 2810–2820, 2013
Keywords: nonlinear systems, fault-tolerant control, model predictive control, process control, process optimization, incipient faults

Introduction

The petrochemical industry worldwide suffers from both large and numerous minor process disturbances and faults that have a significant accumulated effect on production outages and excess energy use over time.[1] Furthermore, the strong interactions between components (i.e., units, actuators, sensors, and controllers) in a chemical process profoundly influence the inherent stability and robustness properties of a closed-loop system and may pose serious reliability, continuity, controllability, and stability issues.[2] In particular, reliability and continuity are important requirements in chemical process industries, which especially apply to complicated safety-critical systems, such as chemical process control systems.[3]

Motivated by the above, the issues of fault-tolerant and fault accommodating controller design have been an active research topic within the chemical process control community over the last decade; see, for example, the book in Ref. 4 and the references therein. Fault-tolerant control methods can be broadly classified into reactive and proactive. Specifically, the traditional approach centers around reactive fault-tolerant control aiming at minimizing the impact of a fault in a process component, actuator or sensor after it occurs, and includes two components: (a) fault detection and isolation (FDI), and (b) reconfiguration of the control system; see, for example, Refs. 4–9 for results in this area. While fault detection and isolation as well as reactive fault-tolerant control schemes remain an active area of research, proactive fault-tolerant control is part of an emerging area that will enable next generation manufacturing (i.e., smart manufacturing/advanced manufacturing). This was pointed out by Bryner[10]: "Today's operations will be transformed from reactive to proactive, response to prevention, …." Proactive fault-tolerant control is emerging as a complement to reactive fault-tolerant control in which appropriate action is taken by the control system before an incipient fault occurs and can help to avoid process shut-down, product loss, and catastrophes involving human and component damage. Specifically, proactive fault-tolerance deals with measures undertaken to predict and minimize the negative impact of future fault situations. It sets up the reconfiguration of control system to avoid the production loss due to the fault and to allow for a smooth transition to postfault control system. Up to this point, however, little work has been done on proactive fault-tolerant control in the context of chemical process control, despite recent industrial calls for moving into this direction. It is important to note at this point that results on proactive and reactive scheduling approaches of chemical multi-product batch plants with uncertain operation times and equipment failures have been developed[11,12] as well as

Correspondence concerning this article should be addressed to Panagiotis D. Christofides at pdc@seas.ucla.edu.
This article had been nominated by AIChE Session Chair, Dr. Jie Yu (McMaster University), as the "Best Presentation" at that session during the AIChE Annual Meeting in Pittsburgh, PA, Oct. 28–Nov. 2, 2012.

that proactive fault-tolerant control technologies have been extensively researched in communication, computer, and aerospace control system communities; see Refs. 5, 13–15 and the references therein.

With respect to the determination of incipient faults, history-based approaches is one of the main types of fault detection and diagnosis techniques that can be used to determine faults.[16,17] Within this framework, large quantities of historical process data are first collected on sensor and actuator faults. The average failure data indicate that components may fail after a certain period of time with a certain probability as their reliability decreases with time.[18] At this point, it is not hard to envision leveraging these data to determine failure windows of process control system components and the best time intervals to schedule preventive process control system maintenance. In terms of the determination of the time of the incipient fault, existing probabilistic prediction methods mainly include methods based on Markov[19] and Bayesian analysis.[20] In detail, multivariate systems can be monitored by building a principal component analysis (PCA) model using historical data. T^2 and sum-of-squared-prediction error (SPE) of the calibration model facilitate fault detection and isolation on-line.[21] In Ref. 20, one-step prediction fault probabilities are estimated by kernel density estimation method according to the statistics corresponding control limits. While these methods of fault determination are used with reactive fault-tolerant control, they could be also used to get an estimate of a time window where a control actuator will likely fail to be used in a proactive fault-tolerant control scheme.

Motivated by the above considerations, in this work, we formulate a proactive fault-tolerant model predictive controller (MPC) designed via Lyapunov-based techniques for nonlinear systems capable of taking proactive measures to minimize the effect of an incipient control actuator fault. Specifically, the proactive fault-tolerant Lyapunov-based MPC (LMPC) is used to take a suspect control actuator out of operation to repair, rebuild, or replace it (e.g., pump rebuild, valve replacement, etc.) while maintaining process operation at desired steady-state. This approach to proactive fault-tolerant control combines the unique stability and robustness properties of LMPC as well as explicitly accounting for an incipient control actuator fault in the formulation of the MPC. We apply our theoretical results to a chemical process example, and different case studies with various types of actuator faults were simulated to demonstrate that the proposed proactive fault-tolerant model predictive control method can achieve practical stability after a control actuator fault.

Preliminaries

Notation

The operator $|\cdot|$ is used to denote the Euclidean norm of a vector and $|\cdot|_Q$ denotes the square of the weighted Euclidean norm of a vector (i.e., $|\cdot|_Q = x^T Q x$). A continuous function $\alpha : [0, a) \to [0, \infty)$ belongs to class $\mathcal{K}$ functions if it is strictly increasing and satisfies $\alpha(0) = 0$. We use Ω_ρ to denote the level set $\Omega_\rho := \{x \in \mathbf{R}^{n_x} | V(x) \leq \rho\}$. The symbol diag (v) denotes a square diagonal matrix with diagonal elements equal to the vector v.

Class of nonlinear systems

In this work, we consider a class of input-affine nonlinear systems described by the following state-space model

$$\dot{x}(t) = f(x(t)) + G_1(x(t))(u(t) + \tilde{u}(t)) + G_2(x(t))w(t) \quad (1)$$

where $x(t) \in \mathbf{R}^n$ is the state vector, $u(t) \in \mathbf{R}^m$ is the manipulated input vector, $\tilde{u}(t) \in \mathbf{R}^m$ is the control actuator fault vector, and $w(t) \in W \subset \mathbf{R}^w$ is the disturbance vector that is bounded by $|w(t)| \leq w_p$. We consider that $u + \tilde{u}$ is bounded in a nonempty convex set $U \subseteq \mathbf{R}^m$ defined as $U := \{u \in \mathbf{R}^m | |u_i + \tilde{u}_i| \leq u_i^{\max}, i = 1, \ldots, m\}$. We assume that $f : \mathbf{R}^n \to \mathbf{R}^n$, $G_1 : \mathbf{R}^n \to \mathbf{R}^n \times \mathbf{R}^m$, and $G_2 : \mathbf{R}^n \to \mathbf{R}^n \times \mathbf{R}^w$ are locally Lipschitz vector and matrix functions, respectively. We use $j = 0$ to denote the fault-free system and $j = 1, \ldots, m$ to denote the system with a fault in the jth control actuator.

We assume that the nominal system of Eq. 1 ($\tilde{u} \equiv 0$) has an equilibrium point at the origin. We also assume that the state x of the system is sampled synchronously and continuously and the time instants where the state measurements become available is indicated by the time sequence $\{t_{k \geq 0}\}$ with $t_k = t_0 + k\Delta$, $k = 0, 1, \ldots$ where t_0 is the initial time and Δ is the sampling time.

Lyapunov-based controller

We assume that there exists a Lyapunov-based controller $u(t) = h_0(x)$ which renders the origin of the fault-free closed-loop system asymptotically stable under continuous implementation. This assumption is essentially a stabilizability requirement for the system of Eq. 1. Furthermore, we assume after the jth control actuator fails that there exists another Lyapunov-based controller $u(t) = h_j(x)$ that renders the origin of the resulting faulty closed-loop system asymptotically stable. Using converse Lyapunov theorems,[22–24] this assumption implies that there exist functions $\alpha_{i,j}(\cdot)$, $i = 1, 2, 3, 4$, $j = 0, 1, 2, \ldots, m$ of class $\mathcal{K}$ and continuous differentiable Lyapunov functions $V_j(x)$ for the closed-loop system that satisfy the following inequalities

$$\alpha_{1,j}(|x|) \leq V_j(x) \leq \alpha_{2,j}(|x|) \quad (2)$$

$$\frac{\partial V_j(x)}{\partial x}\left(f(x) + G_1(x)h_j(x)\right) \leq -\alpha_{3,j}(|x|) \quad (3)$$

$$\left|\frac{\partial V_j(x)}{\partial x}\right| \leq \alpha_{4,j}(|x|) \quad (4)$$

$$h_j(x) \in U_j \quad (5)$$

for all $x \in D \subseteq \mathbf{R}^n$ where D is an open neighborhood of the origin. We denote the region $\Omega_{\rho_j} \subseteq D$ as the stability region of the closed-loop system under the control $u = h_j(x)$. Note that explicit stabilizing control laws that provide explicitly defined stability regions Ω_{ρ_j} for the closed-loop system have been developed using Lyapunov techniques for input-affine nonlinear systems; see Refs. 25–27.

We assume that after some time t_f the jth control actuator fails or the reliability of the actuator has decreased to a level that it becomes desirable to replace or repair the actuator. This time can be estimated from historical life cycle data of the actuator or based on when preventive maintenance is scheduled to be performed on the actuator. We note that there exists a horizon $t_f - t_0$ sufficiently large such that the controller $h_0(x)$ can force the system into the stability region Ω_{ρ_j} by the time t_f starting from any initial state $x(t_0) \in \Omega_{\rho_0}$ (more precisely, it will drive the system to the intersection between Ω_{ρ_j} and Ω_{ρ_0}). We also assume that $V_0 = V_1 = \cdots = V_m = V$.

By continuity and the local Lipschitz property assumed for the vector fields, the manipulated input u is bounded in a

convex set, and the continuous differentiable property of the Lyapunov function V, there exist positive constants M, L_x, and L_w such that

$$|f(x) + G_1(x)(u + \tilde{u}) + G_2(x)w| \leq M \tag{6}$$

$$\left|\frac{\partial V}{\partial x}(f(x) + G_1(x)(u + \tilde{u}) + G_2(x)w(t)) - \frac{\partial V}{\partial x}(f(x') + G_1(x')(u + \tilde{u}))\right| \leq L_x|x - x'| + L_w|w| \tag{7}$$

for all $x, x' \in \Omega_{\rho_j}$, $u + \tilde{u} \in U$, and $w \in W$.

Remark 1. For input-affine nonlinear systems arising in the context of chemical process control applications, weighted Euclidean norm Lyapunov functions (i.e., $V(x) = x^T(t)Px(t)$) have been widely used; see Ref. 25 and the references therein. See the Application to a Chemical Process section for an example.

Remark 2. The assumption that there exists a controller $h_j(x)$ that stabilizes the faulty system is a necessary requirement. Typically, this can be accomplished in chemical process control in one of two ways: (1) the principle of redundancy is used in fault-tolerant systems to ensure stability after a fault (i.e., if a control actuator fails, there is another actuator that can be used to maintain stability), and (2) many chemical processes are designed to be open-loop asymptotically stable so the failure of a control actuator does not affect the stability of the closed-loop system.

Remark 3. We note that there is no guarantee that the stability region Ω_{ρ_j} of the faulty system is a subset of the fault-free stability region Ω_{ρ_0} because the controllers $h_0(x)$ and $h_j(x)$ can be different. We do know that the two regions intersect in a neighborhood of the origin and it is this intersection that we use in our design of the proactive fault-tolerant controller.

Remark 4. We note that implementing the proactive fault-tolerant LMPC for preventive maintenance does not require that we accurately predict the time the actuator will fail, but rather, we estimate a time window that the actuator reaches the end of its life cycle and no longer becomes reliable. In this case, we would use the most conservative or earliest estimate and the LMPC would consider that as the time of the incipient fault. As we demonstrate in the example, the proactive fault-tolerant LMPC also operates the process optimally from a cost index perspective.

Proactive Fault-tolerant MPC

In this section, we introduce the proposed proactive fault-tolerant Lyapunov-based model predictive controller and prove practical stability of the closed-loop system of Eq. 1 with the proactive fault-tolerant LMPC.

Implementation strategy

The implementation strategy of the proposed proactive fault-tolerant LMPC is represented by Figure 1. Specifically, from t_0 to t_f, the LMPC with sampling period Δ and prediction horizon N starts from an initial condition in the stability region Ω_{ρ_0} and recomputes optimal control actions at every sampling period by solving an on-line optimization problem while accounting for the actuator fault that occurs at t_f. It does so by working to drive the system into the stability region Ω_{ρ_j} by the time t_f (the time of the fault). After the fault renders the jth actuator inactive, the proactive fault-tolerant LMPC drives the system to the origin using its available (remaining) $m-1$ actuators. The implementation strategy steps of the proposed proactive fault-tolerant LMPC can be summarized as follows:

1. At t_k, the proactive fault-tolerant LMPC receives the process state from the sensors;
2. If $t_{k+1} < t_f$ (the time of the fault), go to Step 2.1; otherwise go to Step 2.2;
   2.1. Compute control actions that account for the fault at t_f and drive the system to the stability region Ω_{ρ_j} by t_f; go to Step 3;
   2.2. Drive the system to the origin with the remaining $m-1$ control actuators; go to Step 3;
3. Go to Step 1, $t_k := t_{k+1}$.

By comparing the time of the fault with the next sampling time (t_{k+1}), the proactive fault-tolerant LMPC completes control system reconfiguration before the fault.

With this implementation strategy, we point out that the key difference between this proactive approach to dealing with actuator faults and traditional reactive fault tolerant control is that when there is a known fault it may be necessary to adjust the control energy to drive the system to the stability region Ω_{ρ_j} before the jth control actuator fails compared to a controller which does not account for an upcoming fault. This guarantees that the remaining $m-1$ control actuators can stabilize the system after the fault occurs. This strategy differs from reactive fault tolerant control that cannot proactively drive the system to a region whereby stability is guaranteed after the jth actuator fails. After a fault occurs and has been identified with reactive fault-tolerant control, the closed-loop system may lose stabilizability of the origin with the remaining control actuators if the closed-loop state is outside the stability region Ω_{ρ_j}.

Remark 5. We note that we are not introducing a fault-tolerant control scheme that can replace classical reactive fault-tolerant control schemes that deal with any type (potentially unexpected) of fault. Instead, the proactive fault-tolerant LMPC is used as an added mechanism to maintain process operation without losing stability and with minimal performance degradation compared to a full plant shutdown while operators carry out maintenance/replace a faulty actuator.

Formulation

We formulate an LMPC based on the conceptual framework proposed in Refs. 22 and 28 for use as a proactive

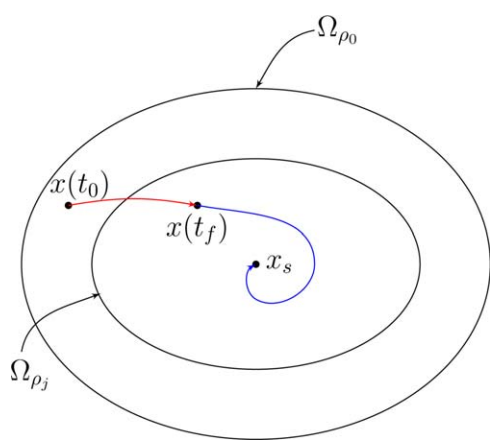

Figure 1. Conceptual diagram of the implementation strategy of proactive fault-tolerant LMPC.

The proactive fault-tolerant LMPC works to drive the system into the stability region Ω_{ρ_j} by the time t_f and uses the remaining $m-1$ actuators to drive the system to the origin after the fault renders the jth actuator inactive. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

fault-tolerant controller. The LMPC is based on the Lyapunov-based controllers $h_0(x)$ and $h_j(x)$ because the controllers are used to define a stability constraint for the LMPC which guarantees that the LMPC inherits the stability and robustness properties of the Lyapunov-based controllers. The proactive fault-tolerant LMPC is based on the following optimization problem

$$\min_{u\in S(\Delta)} \int_{t_k}^{t_{k+N}} \left[|\tilde{x}(\tau)|_{Q_c} + |u(\tau)|_{R_c} \right] d\tau \tag{8a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t)) + G_1(\tilde{x}(t))(u(t) + \tilde{u}(t)) \tag{8b}$$

$$u(t) \in U \tag{8c}$$

$$\tilde{u}_j(t) = \begin{cases} 0, & \text{if} \quad t < t_{\rm f} \\ -u_j(t), & \text{if} \quad t \geq t_{\rm f} \end{cases} \tag{8d}$$

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

$$\frac{\partial V}{\partial x}(f(x(t_k)) + G_1(x(t_k))u(t_k)) \leq \frac{\partial V}{\partial x}(f(x(t_k)) + G_1(x(t_k))h_0(x(t_k))), \quad \text{if} \quad t_{k+1} < t_{\rm f}, \tag{8f}$$

$$\frac{\partial V}{\partial x}(f(x(t_k)) + G_1(x(t_k))u(t_k)) \leq \frac{\partial V}{\partial x}(f(x(t_k)) + G_1(x(t_k))h_j(x(t_k))), \quad \text{if} \quad t_{k+1} \geq t_{\rm f} \tag{8g}$$

where $S(\Delta)$ is the family of piece-wise constant functions with sampling period Δ, N is the prediction horizon of the LMPC, $\tilde{u}(t)$ is the actuator fault trajectory, $\tilde{x}(t)$ is the state trajectory predicted by the nominal model $(w(t) \equiv 0)$ with manipulated input $u(t)$ computed by the LMPC. The optimal solution of the optimization problem of Eq. 8 is denoted by $u^*(t|t_k)$ and is defined for $t \in [t_k, t_{k+N})$.

In the optimization problem of Eq. 8, the first constraint of Eq. 8b is the nonlinear system of Eq. 1 used to predict the future evolution of the system. The constraint of Eq. 8c defines the control energy available to all manipulated inputs. The constraint of Eq. 8d is the complete fault of the jth control actuator that causes the actuator to be unusable for $t \geq t_{\rm f}$. The constraint of Eq. 8e is the initial condition of the optimization problem. The constraints of Eq. 8f and 8g ensure that over the sampling period $t \in [t_k, t_k + \Delta)$, the LMPC computes a manipulated input that decreases the Lyapunov function by at least the rate achieved by the Lyapunov-based controllers $h_0(x)$ when $t_{k+1} < t_{\rm f}$ and $h_j(x)$ when $t_{k+1} \geq t_{\rm f}$ when the Lyapunov-based controllers are implemented in a sample-and-hold fashion. We note that in the optimization problem of Eq. 8, the time instance that is used to determine which Lyapunov-based constraint to use is t_{k+1} to account for a fault that may occur between two sampling times. In this manner, the controller is proactively regulating the closed-loop system trajectory.

Stability analysis

In this section, we provide sufficient conditions whereby the proactive fault-tolerant controller of Eq. 8 guarantees practical stability of the closed-loop system. Theorem 1 below provides sufficient conditions such that the proactive fault-tolerant LMPC guarantees that the state of the closed-loop system is always bounded and is ultimately bounded in a small region containing the origin.

Theorem 1. Consider the system in closed-loop under the proactive fault-tolerant LMPC design of Eq. 8 based on controllers $h_j(x)$, $j = 0, 1, \ldots, m$ that satisfies the conditions of Eqs. 2–5. Let $\Delta > 0$, $\epsilon_0 > 0$, $\rho_0 > \rho_{s,0} > 0$, $\epsilon_j > 0$, and $\rho_j > \rho_{s,j} > 0$ satisfy

$$-\alpha_{3,0}\left(\alpha_{2,0}^{-1}(\rho_{s,0})\right) + L_x M\Delta + L_w w_{\rm p} \leq -\epsilon_0/\Delta \tag{9}$$

$$-\alpha_{3,j}\left(\alpha_{2,j}^{-1}(\rho_{s,j})\right) + L_x M\Delta + L_w w_{\rm p} \leq -\epsilon_j/\Delta \tag{10}$$

If $x(t_0) \in \Omega_{\rho_0}$, $\rho_{\min} \leq \rho_j$ and $t_{\rm f} - t_0$ is sufficiently large such that $x(t_{\rm f}) \in \Omega_{\rho_j}$, then the state $x(t)$ of the closed-loop system is always bounded and is ultimately bounded in $\Omega_{\rho_{\min}}$ where $\rho_{\min} = \max\{V(x(t+\Delta)) : V(x(t)) \leq \rho_{s,j}\}$.

Proof. The proof consists of three parts. We first prove that the optimization problem is feasible. Subsequently, we prove that, under the LMPC design, the closed-loop state of the system is always bounded and will converge to a small set containing the origin after a finite number of sampling periods. Finally, we prove that under the LMPC, the closed-loop state of the system is ultimately bounded in the set $\Omega_{\rho_{\min}}$.

Part 1. When $x(t)$ is maintained in Ω_{ρ_0} for $t < t_{\rm f}$ and in Ω_{ρ_j} for $t \geq t_{\rm f}$ (which will be proved in Part 2), the feasibility of the LMPC follows because the input trajectory $u(t) = h_j(x(t_{k+q}))$, $\forall t \in [t_{k+q}, t_{k+q+1})$ with $q = 0, \ldots, N-1$ ($j = 0$ for $t < t_{\rm f}$) is a feasible solution to the optimization problem as such a trajectory satisfies the input constraint and the Lyapunov-based constraints. This is guaranteed by the closed-loop stability property of the Lyapunov-based controllers $h_0(x)$ and $h_j(x)$.

Part 2. We prove that if $x(t_k) \in \Omega_{\rho_0} \backslash \Omega_{\rho_{s,0}}$ and $t_{k+1} < t_{\rm f}$, then $V(x(t_{k+1})) < V(x(t_k))$ and after a finite time, either the system will converge to the set $\Omega_{\rho_{s,0}}$, which is contained in the set Ω_{ρ_j}, or it will converge to the set $\Omega_{\rho_0} \cap \Omega_{\rho_j}$ by $t_{\rm f}$.

When $x(t_k) \in \Omega_{\rho_0} \backslash \Omega_{\rho_{s,0}}$ and $t_{k+1} < t_{\rm f}$, from the last constraint of the LMPC of Eq. 8 and accounting for Eq. 3, the derivative of the Lyapunov function along the system trajectory at t_k is

$$\frac{\partial V(x(t_k))}{\partial x}(f(x(t_k)) + G_1(x(t_k))u^*(t_k)) \leq \frac{\partial V(x(t_k))}{\partial x} \times (f(x(t_k)) + G_1(x(t_k))h_0(x(t_k))) \leq -\alpha_{3,0}(|x(t_k)|) \tag{11}$$

The time derivative of the Lyapunov function along the computed optimal trajectories u^* for $\forall \tau \in [t_k, t_{k+1})$ can be written as follows

$$\dot{V}(x(\tau)) = \frac{\partial V(x(\tau))}{\partial x}(f(x(\tau)) + G_1(x(\tau))u^*(t_k) + G_2(x(\tau))w(t)) \tag{12}$$

Adding and subtracting the term $\frac{\partial V(x(t_k))}{\partial x}(f(x(t_k)) + G(x(t_k))u^*(t_k))$ to/from the above equation and considering the bound of Eq. 11, we have

$$\dot{V}(x(\tau)) \leq -\alpha_{3,0}(|x(t_k)|) - \frac{\partial V}{\partial x}(f(x(t_k)) + G_1(x(t_k))u^*(t_k)) + \frac{\partial V}{\partial x}(f(x(\tau)) + G_1(x(\tau))u^*(t_k) + G_2(x(\tau))w(\tau)) \tag{13}$$

From the Lipschitz property of Eq. 7 and accounting for the bounded disturbance, we can write

$$\dot{V}(x(\tau)) \leq -\alpha_{3,0}(|x(t_k)|) + L_x|x(\tau) - x(t_k)| + L_w w_{\rm p} \tag{14}$$

Taking into account Eq. 6 and the continuity of $x(t)$, the following bound can be written for all $\tau \in [t_k, t_{k+1})$

$$|x(\tau)-x(t_k)| \leq M\Delta \tag{15}$$

Using the bound of Eq. 15 and as $x(t_k) \in \Omega_{\rho_0} \backslash \Omega_{\rho_{s,0}}$, the bound of Eq. 14 becomes

$$\dot{V}(x(\tau)) \leq -\alpha_{3,0}\left(\alpha_{2,0}^{-1}(\rho_{s,0})\right) + L_x M\Delta + L_w w_p \tag{16}$$

If the condition of Eq. 9 is satisfied, then there exists $\epsilon_0 > 0$ such that the following inequality holds for $x(t_k) \in \Omega_{\rho_0} \backslash \Omega_{\rho_{s,0}}$

$$\dot{V}(x(t)) \leq -\epsilon_0/\Delta, \forall t = [t_k, t_{k+1}) \tag{17}$$

Integrating this bound on $t \in [t_k, t_{k+1})$, we obtain that

$$\begin{aligned} V(x(t_{k+1})) &\leq V(x(t_k)) - \epsilon_0 \\ V(x(t)) &\leq V(x(t_k)), \qquad \forall t \in [t_k, t_{k+1}) \end{aligned} \tag{18}$$

for all $x(t_k) \in \Omega_{\rho_0} \backslash \Omega_{\rho_{s,0}}$. Using Eq. 18 recursively, it is proved that, if $x(t_k) \in \Omega_{\rho_0} \backslash \Omega_{\rho_{s,0}}$, the state converges to $\Omega_{\rho_{s,0}} \subset \Omega_{\rho_0}$ in a finite number of sampling times without leaving the stability region Ω_{ρ_0}.

The horizon $(t_f - t_0)$ is chosen to be sufficiently large such that starting from any $x(t_0) \in \Omega_{\rho_0}$, the state will be driven into the set Ω_{ρ_j} by t_f. Similar arguments as above can be used to show that after t_f, operation is always maintained in the set Ω_{ρ_j} and converges to the set $\Omega_{\rho_{s,j}} \subset \Omega_{\rho_j}$ after some finite number of sampling periods if the conditions of Eq. 10 are satisfied.

Part 3. We prove that if $x(t_k) \in \Omega_{\rho_j}$ for $t_k \geq t_f$, then the system state will ultimately be bounded in an invariant set $\Omega_{\rho_{\min}}$. From Part 2, we proved that if $x(t_0) \in \Omega_{\rho_0}$, the state converges to Ω_{ρ_j} before t_f and after a finite number of sampling times, the system will be driven to the set $\Omega_{\rho_{s,j}}$. Once the state converges to $\Omega_{\rho_{s,j}}$, it remains inside $\Omega_{\rho_{\min}}$ for all times. This statement holds because of the definition of $\rho_{\min}$. This proves that the closed-loop system state under the LMPC of Eq. 8 is ultimately bounded in $\Omega_{\rho_{\min}}$.

Remark 6. We note that in many realistic actuator faults, a fault is initially gradual meaning that the maximum available actuator output decreases slowly with time until the maximum output begins to drastically decrease (sigmoid relationship). In this manner, the bounds on the available actuator output become time-dependent. This is a mild extension of what is covered in the stability proof. As long as the evolution of the constraint set is a known function of time *a priori*, the time-dependent bound may be used in the LMPC formulation. From a stability point of view, the goal of the proactive fault-tolerant controller is to drive the closed-loop system to the stability region without the faulty control actuator Ωj by the time the fault starts whether that fault is abrupt or gradual. If this is accomplished at the time of the fault, then we can guarantee closed-loop stability. This follows from a simple argument that if we can stabilize the system with $m-1$ actuators, we can also stabilize with $m-1$ plus the gradually decaying one. This remark refers to case B in our application of this theory to a chemical process in the next section, where this type of fault is implemented and handled.

Application to a Chemical Process

Consider a three vessel, reactor-separator chemical process consisting of two CSTRs in series followed by a flash tank separator as shown in Figure 2. Two parallel first-order reactions occur in each of the reactors that have the form

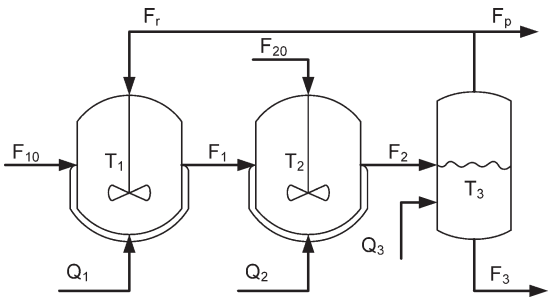

Figure 2. Process flow diagram of the reactor and separator chemical process.

$$A \xrightarrow{r_1} B$$

$$A \xrightarrow{r_2} C$$

Each reactor is supplied with a fresh stream of the reactant A contained in an inert solvent D. A recycle stream is used to recover unreacted A from the overhead vapor of the flash tank and feed it back to the first CSTR. Some of the overhead vapor from the flash tank is condensed, and the bottom product stream is removed. All three vessels are assumed to have static holdup and are equipped with a jacket to supply/remove heat from the vessel. The dynamic equations describing the behavior of the system, obtained through material and energy balances under standard modeling assumptions, are given below

$$\frac{dT_1}{dt} = \frac{F_{10}}{V_1}(T_{10}-T_1) + \frac{F_r}{V_1}(T_3-T_1) + \frac{-\Delta H_1}{\rho C_p} k_1 e^{\frac{-E_1}{RT_1}} C_{A1} + \frac{-\Delta H_2}{\rho C_p} k_2 e^{\frac{-E_2}{RT_1}} C_{A1} + \frac{Q_1}{\rho C_p V_1} \tag{19}$$

$$\frac{dC_{A1}}{dt} = \frac{F_{10}}{V_1}(C_{A10}-C_{A1}) + \frac{F_r}{V_1}(C_{Ar}-C_{A1}) - k_1 e^{\frac{-E_1}{RT_1}} C_{A1} - k_2 e^{\frac{-E_2}{RT_1}} C_{A1} \tag{20}$$

$$\frac{dC_{B1}}{dt} = \frac{-F_{10}}{V_1} C_{B1} + \frac{F_r}{V_1}(C_{Br}-C_{B1}) + k_1 e^{\frac{-E_1}{RT_1}} C_{A1} \tag{21}$$

$$\frac{dC_{C1}}{dt} = \frac{-F_{10}}{V_1} C_{C1} + \frac{F_r}{V_1}(C_{Cr}-C_{C1}) + k_2 e^{\frac{-E_2}{RT_1}} C_{A1} \tag{22}$$

$$\frac{dT_2}{dt} = \frac{F_1}{V_2}(T_1-T_2) + \frac{F_{20}}{V_2}(T_{20}-T_2) + \frac{-\Delta H_1}{\rho C_p} k_1 e^{\frac{-E_1}{RT_2}} C_{A2} + \frac{-\Delta H_2}{\rho C_p} k_2 e^{\frac{-E_2}{RT_2}} C_{A2} + \frac{Q_2}{\rho C_p V_2} \tag{23}$$

$$\frac{dC_{A2}}{dt} = \frac{F_1}{V_2}(C_{A1}-C_{A2}) + \frac{F_{20}}{V_2}(C_{A20}-C_{A2}) - k_1 e^{\frac{-E_1}{RT_2}} C_{A2} - k_2 e^{\frac{-E_2}{RT_2}} C_{A2} \tag{24}$$

$$\frac{dC_{B2}}{dt} = \frac{F_1}{V_2}(C_{B1}-C_{B2}) - \frac{F_{20}}{V_2} C_{B2} + k_1 e^{\frac{-E_1}{RT_2}} C_{A2} \tag{25}$$

$$\frac{dC_{C2}}{dt} = \frac{F_1}{V_2}(C_{C1}-C_{C2}) - \frac{F_{20}}{V_2} C_{C2} + k_2 e^{\frac{-E_2}{RT_2}} C_{A2} \tag{26}$$

$$\frac{dT_3}{dt} = \frac{F_2}{V_3}(T_2-T_3) - \frac{H_{vap} F_{rm}}{\rho C_p V_3} + \frac{Q_3}{\rho C_p V_3} \tag{27}$$

$$\frac{dC_{A3}}{dt} = \frac{F_2}{V_3}(C_{A2}-C_{A3}) - \frac{F_r}{V_3}(C_{Ar}-C_{A3}) \tag{28}$$

Table 1. Notation Used for the Process Parameters and Variables

C_{Aj0}	Concentration of A in the feed stream to vessel j, $j=1,2$
$C_{i,j}$	Concentration of species i, $i=A,B,C$ in vessel j, $j=1,2,3$
$C_{i,r}$	Concentration of species i, $i=A,B,C$ in the recycle stream
T_{j0}	Temperature of the feed stream to vessel j, $j=1,2$
T_j	Temperature in vessel j, $j=1,2,3$
T_r	Temperature in the recycle stream
F_{j0}	Flow rate of the feed stream to vessel j, $j=1,2$
F_j	Flow rates of the effluent stream from vessel j, $j=1,2,3$
F_r	Flow rate of the recycle stream
F_p	Flow rate of the purge stream
V_j	Volumes of vessel j, $j=1,2,3$
E_k	Activation energy of reaction k, $k=1,2$
k_k	Pre-exponential factor of reaction k, $k=1,2$
ΔH_k	Heat of reaction k, $k=1,2$
H_{vap}	Heat of vaporization
α_i	Relative volatilities of species i, $i=A,B,C,D$
MW_j	Molecular weights of species i, $i=A,B,C,D$
C_p	Heat capacity
R	Gas constant

$$\frac{dC_{B3}}{dt} = \frac{F_2}{V_3}(C_{B2}-C_{B3}) - \frac{F_r}{V_3}(C_{Br}-C_{B3}) \tag{29}$$

$$\frac{dC_{C3}}{dt} = \frac{F_2}{V_3}(C_{C2}-C_{C3}) - \frac{F_r}{V_3}(C_{Cr}-C_{C3}) \tag{30}$$

where the notations are defined in Table 1 and the process parameter values are given in Table 2.

To model the separator, we assume that the relative volatility of each species remains constant within the operating temperature range of the flash tank and that the amount of reacting material in the separator is negligible. The following algebraic equations model the composition of the overhead stream of the separator

$$C_{Ar} = \frac{\alpha_A C_{A3}}{K}, C_{Br} = \frac{\alpha_B C_{B3}}{K}, C_{Cr} = \frac{\alpha_C C_{C3}}{K} \tag{31}$$

$$K = \alpha_A C_{A3}\frac{MW_A}{\rho} + \alpha_B C_{B3}\frac{MW_B}{\rho} + \alpha_C C_{C3}\frac{MW_C}{\rho} + \alpha_D x_D \rho \tag{32}$$

$$F_{rm} = \frac{F_r}{MW_D}[\rho - C_{A3}MW_A - C_{B3}MW_B - C_{C3}MW_C + (C_{A3}+C_{B3}+C_{C3})MW_D] \tag{33}$$

where x_D is the mass fraction of the solvent in the flash tank liquid holdup and F_{rm} is the recycle molar flow rate.

The process has four manipulated input variables: the heat supplied/removed for each vessel and the inlet flow rate F_{20} to the second reactor. The available control energy is $|Q_i| \leq 3\times10^5$ kJ/h, $i=1,2,3$ and $0 \leq F_{20} \leq 10\,m^3/h$. The control objective we consider is to drive the system to the unstable steady-state

$$x_s^T = [T_1 \quad C_{A1} \quad C_{B1} \quad C_{C1} \quad T_2 \quad C_{A2} \quad C_{B2} \quad C_{C2} \quad T_3 \quad C_{A3} \quad C_{B3} \quad C_{C3}]$$
$$= [370 \quad 3.32 \quad 0.17 \quad 0.04 \quad 435 \quad 2.75 \quad 0.45 \quad 0.11 \quad 435 \quad 2.88 \quad 0.50 \quad 0.12]$$

while proactively accounting for an incipient fault under the various simulated control actuator faults.

To design the Lyapunov-based controller $h(x)$, we consider a quadratic Lyapunov function $V(x)=x^TPx$ with $P=\text{diag}([20\,10^3\,10^3\,10^3\,10\,10^3\,10^3\,10^3\,10\,10^3\,10^3\,10^3])$ and design the controller $h(x)$ as three PI controllers with proportional gains $K_{p1}=5000, K_{p2}=7000, K_{p3}=7000$ and integral time constants $\tau_{I1}=\tau_{I2}=\tau_{I3}=10$ based on the deviation of temperature measurements of T_1, T_2, and T_3 from their respective steady-state temperature values. The feed flow rate into the second reactor is set to be a constant $F_{20}=5\,m^3/h$ in the controller $h(x)$. The auxiliary controller $h(x)$ is used in the design of a proactive fault-tolerant LMPC of Eq. 8 with weighting matrices chosen to be $Q_c=P$, $R=\text{diag}([5\times10^{-12} \quad 5\times10^{-12} \quad 5\times10^{-12} \quad 100])$, prediction horizon $N=6$, and sampling period $\Delta=0.005\,h=18s$.

We implement the proactive fault-tolerant LMPC on the reactor-separator chemical process of Eqs. 19–33. To compare the proactive fault-tolerant controller with the closed-loop system without proactive fault-tolerant control, we implement another LMPC that does not account for the fault. The reactor-separator system is initialized at the stable steady-state $T_1=T_2=T_3=301K$, $C_{A1}=3.58$, $C_{A2}=3.33$, $C_{A3}=3.50$, $C_{B1}=C_{B2}=C_{B3}=0$, and $C_{C1}=C_{C2}=C_{C3}=0$. The simulations were carried out using Java programming language in a Intel® Core™ i7, 3.40 GHz computer. The optimization problems were solved using the open source interior point optimization software Ipopt.[29]

In terms of fault/failure, they can be classified by its degree and action time, so we introduce different types of actuator faults in the system. In case study A, we conduct a simulation for a fault in Q_2, which is a complete fault in the corresponding actuator. To simulate a realistic gradual actuator fault, we model a fault in Q_2 as a logistic function in case B as well as introduce process noise into the system. In case C, we simulate process recovery from the faulty system back to the fault-free system with the proposed proactive fault-tolerant controller after the faulty actuator is repaired. The following case studies were completed to simulate these scenarios and demonstrate the practical stability of the closed-loop system of Eqs. 19–33 with the proposed proactive fault-tolerant LMPC.

Complete fault on the heat input to the second reactor

We consider a fault in the heat supplied to/removed from CSTR2 that renders $Q_2=0$ for $t \geq 0.0545h$. The results of

Table 2. Process Parameter Values

$T_{10}=300$, $T_{20}=300$	K
$F_{10}=5$, $F_r=1.9$, $F_p=0$	m^3/h
$C_{A10}=4$, $C_{A20}=3$	$kmol/m^3$
$V_1=1.0$, $V_2=0.5$, $V_3=1.0$	m^3
$E_1=5\times10^4$, $E_2=5.5\times10^4$	kJ/kmol
$k_1=3\times10^6$, $k_2=3\times10^6$	1/h
$\Delta H_1=-5\times10^4$, $\Delta H_2=-5.3\times10^4$	kJ/kmol
$H_{vap}=5$	kJ/kmol
$C_p=0.231$	kJ/kg-K
$R=8.314$	kJ/kmol-K
$\rho=1000$	kg/m^3
$\alpha_A=2$, $\alpha_B=1$, $\alpha_C=1.5$, $\alpha_D=3$	Unitless
$MW_A=MW_B=MW_C=50$, $MW_D=18$	kg/kmol

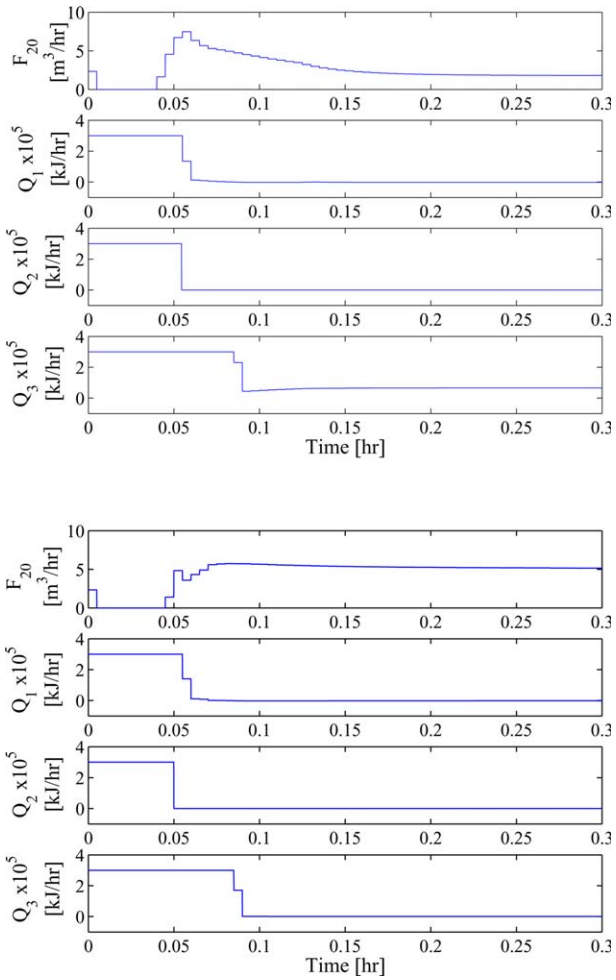

Figure 3. The closed-loop input trajectories.

(a) without proactive fault-tolerant control and (b) with the proposed proactive fault-tolerant LMPC. The fault renders $Q_2(t) = 0$ for $t \geq 0.0545$ h. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

two one-hour closed-loop simulations are shown in Figures 6 and 7. Figure 6 shows the closed-loop process evolution with LMPC but without accounting for the fault and Figure 7 shows the closed-loop process evolution with the proposed proactive fault-tolerant LMPC. Figure 3 shows a plot of the manipulated input trajectories for (a) the closed-loop process without accounting for the fault and (b) the closed-loop process with the proposed proactive fault-tolerant LMPC from $t = 0$ h to $t = 0.3$ h to better highlight the differences between the two types of controllers.

From Figure 3, we observe that the proactive fault-tolerant LMPC feeds less cold reactant by reducing the inlet feed F_{20} into CSTR2 leading up to the fault compared to the closed-loop process without proactive fault-tolerant control. Before the fault, CSTR2 is rich with the reactant A and the temperature in the reactor is less than the desired set-point. Considering that the reaction is exothermic and the initial temperature of inlet feed F_{20}, T_{20}, is colder relative to the desired temperature of CSTR2, the proactive fault-tolerant controller takes advantage of the heat generated from the exothermic reaction to heat the contents of CSTR2. Furthermore, we see that the proactive fault-tolerant controller shuts off the manipulated input Q_2 at the sampling time before the fault occurs and uses only the feed flow F_{20} into CSTR2 to bring the temperature and species concentrations of CSTR2 close to the desired set-points with $Q_2 = 0$. From Figures 6 and 7, the post-fault behavior of these two control strategies is observed. The closed-loop process without proactive fault-tolerant control settles on an offsetting steady-state; whereas, the closed-loop process with the proposed proactive fault-tolerant LMPC settles at the desired steady-state. To compare the closed-loop performance of the two simulations, we use the total closed-loop performance index defined as

$$J = \int_{t=0}^{t=1\text{h}} |x(\tau) - x_s|_{Q_c} + |u(\tau) - u_s|_{R_c} d\tau \tag{34}$$

of each simulation. The total performance index with the proposed proactive fault-tolerant LMPC is 2.35×10^4 which is an order of magnitude smaller than 1.99×10^5 which is the total closed-loop process performance index with the LMPC that does not account for the fault.

Gradual fault on the heat input to the second reactor

In certain cases, an actuator may fail gradually. Based on the empirical function of the reliability of process components, the maximum available output of the faulty actuator usually decreases exponentially on the basis of its original maximum available output.[30] Thus, in this case, we use a logistic function to represent the maximum available output of the faulty actuator for the heat input/removal to CSTR2. The logistic function has a general formula as follows[31]

$$|U_{\max}(t)| = \frac{a}{1 + \exp\left(\frac{-(t-c)}{b}\right)} |U_{\max,0}| \tag{35}$$

where a, b and c are parameters, $|U_{\max}(t)|$ is the maximum available control energy of the jth faulty control actuator, and $|U_{\max,0}|$ is the maximum available output of the actuator under fault-free conditions. Figure 4 shows a plot of the logistic function of Eq. 35 used to model a gradual fault in Q_2 with parameters: $a = 1$, $b = -0.01$ h and $c = 0.055$ h. From the plot, we can observe that the maximum available output value decreases slowly at the beginning, but the

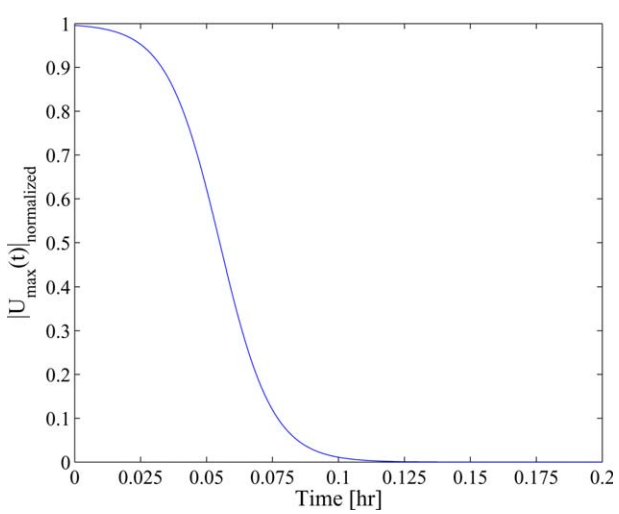

Figure 4. The plot of the logistic function for the normalized maximum output of the faulty actuator.

At $t = 0.1$ h, the maximum output of the faulty actuator becomes very close to 0% of its fault-free output value. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

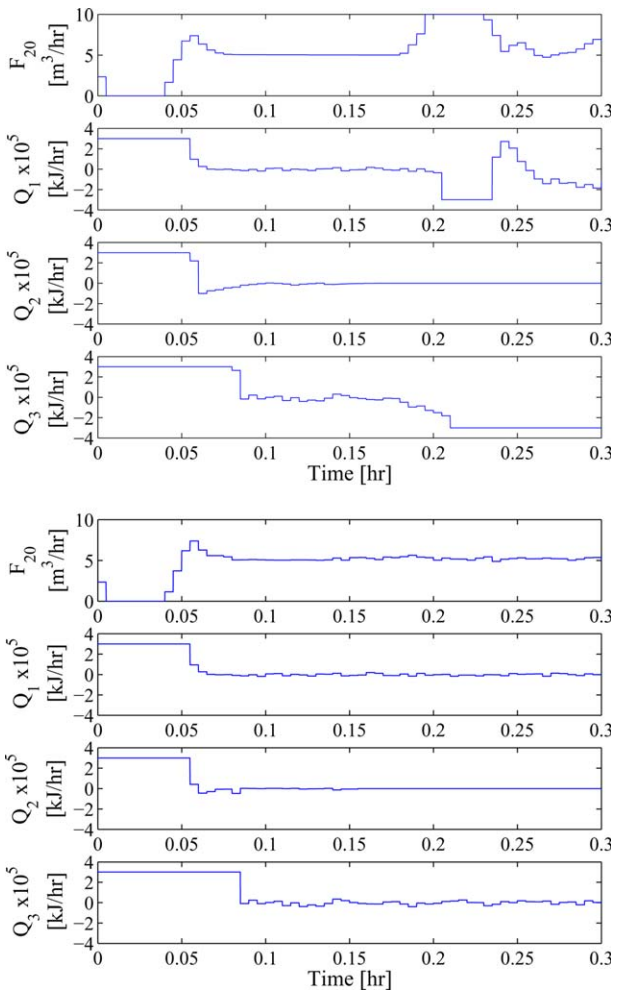

Figure 5. The closed-loop input trajectories.

(a) without proactive fault-tolerant control and (b) with the proposed proactive fault-tolerant LMPC. The maximum available control energy in the faulty actuator of Q_2 follows the logistic function of Eq. 35 with parameters: $a = 1$, $b = -0.01$ h and $c = 0.055$ h; the gradual fault starts at $t = 0.0545$ h. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

derivative of this function decreases quickly which is characteristic of a realistic actuator fault. For this particular function, the maximum available output of the faulty actuator becomes very close to 0% of its fault-free output at $t = 0.1$ h.

Instead of switching the control problem from four control actuators to the three remaining control actuators at the beginning of the gradual fault, the proactive fault-tolerant LMPC accounts for the faulty actuator of Q_2 whose maximum available output decreases following the above logistic function. In this case, the gradual fault begins at $t = 0.0545$ h and the proactive fault-tolerant LMPC regards $t = 0.1545$ h as the time to reconfigure the control system from four available control actuators to the three remaining control actuators. This time has been chosen as 0.1h after the beginning of the gradual fault because the maximum available output of the faulty actuator at this time is almost 0% of its fault-free output.

We also consider the effect of bounded process noise on the process. Process noise is added to each of the 12 states and modeled as bounded Gaussian white noise with 0 mean, unit variance, and bounds given by $w_p = [2\ 0.25\ 0.05\ 0.05\ 2\ 0.25\ 0.05\ 0.05\ 2\ 0.25\ 0.05\ 0.05]$. The results of two one-hour closed-loop simulations are shown in Figures 8 and 9. Figure 8 shows the closed-loop process evolution with LMPC, but without accounting for the fault and Figure 9 shows the closed-loop process evolution with the proposed proactive fault-tolerant LMPC. Figure 5 shows a plot of the manipulated input trajectories for (a) the closed-loop process

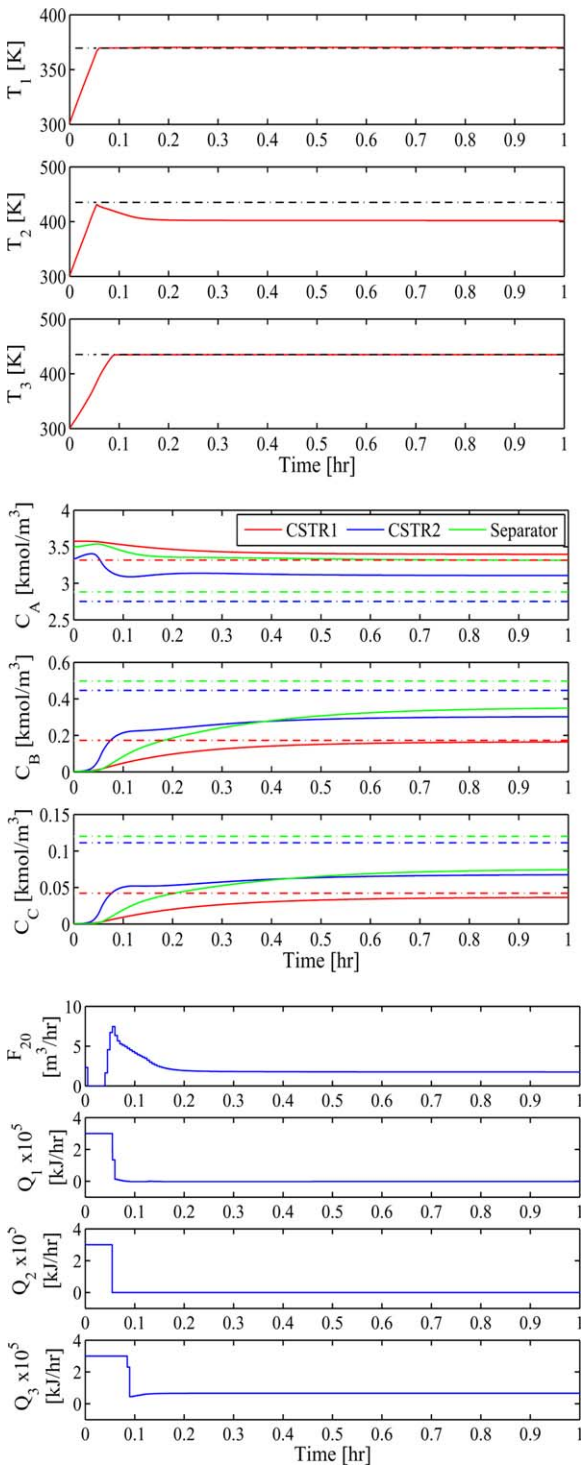

Figure 6. The closed-loop process state and manipulated input trajectories (solid lines) and set-points (dashed lines).

(a) vessel temperatures, (b) species concentrations, (c) manipulated inputs without proactive fault-tolerant control applied. The fault renders $Q_2(t) = 0$ for $t \geq 0.0545$ h. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

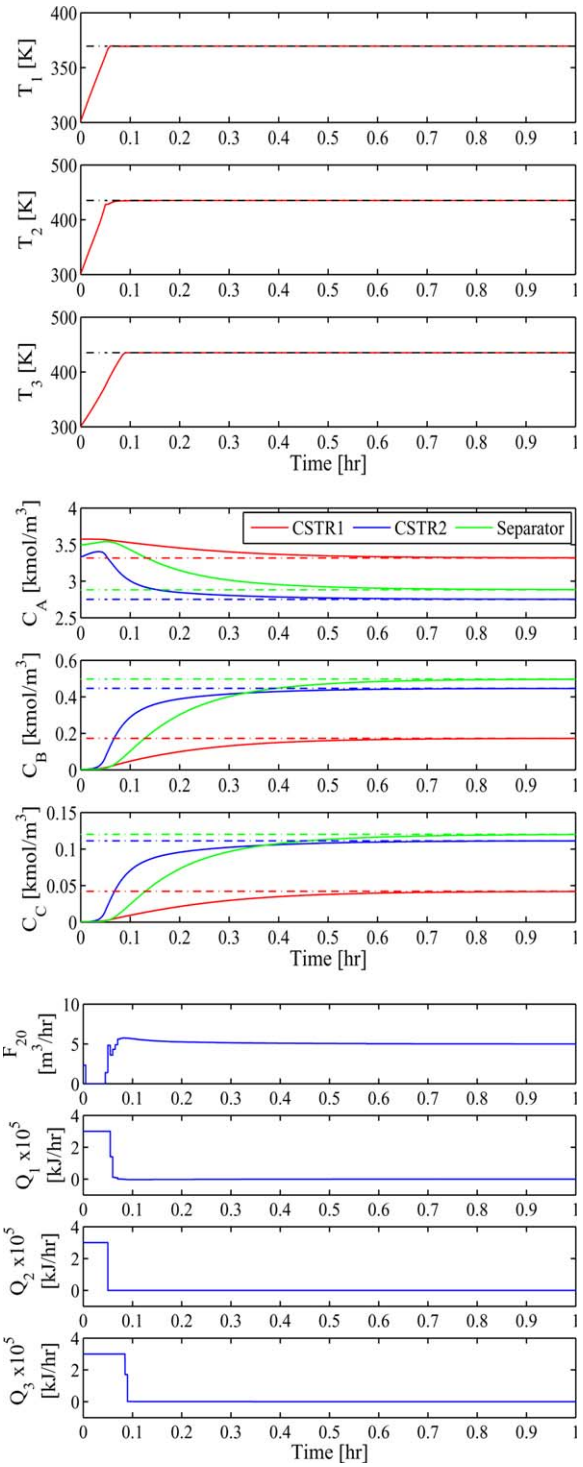

Figure 7. The closed-loop process state and manipulated input trajectories (solid lines) and set-points (dashed lines).

(a) vessel temperatures, (b) species concentrations, (c) manipulated inputs with proactive fault-tolerant control applied. The fault renders $Q_2(t) = 0$ for $t \geq 0.0545$ h. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

without accounting for the fault and (b) the closed-loop process with the proposed proactive fault-tolerant LMPC from $t = 0$ h to $t = 0.3$ h to better highlight the differences between the two types of controllers. The maximum available control energy in the faulty actuator of Q_2 follows the logistic function of Eq. 35 with the parameters $a = 1$, $b = -0.01$ h and $c = 0.055$ h. The gradual fault begins at $t = 0.0545$ h.

From Figure 3b, we observe that the proactive fault-tolerant controller chooses a similar strategy as in case A.

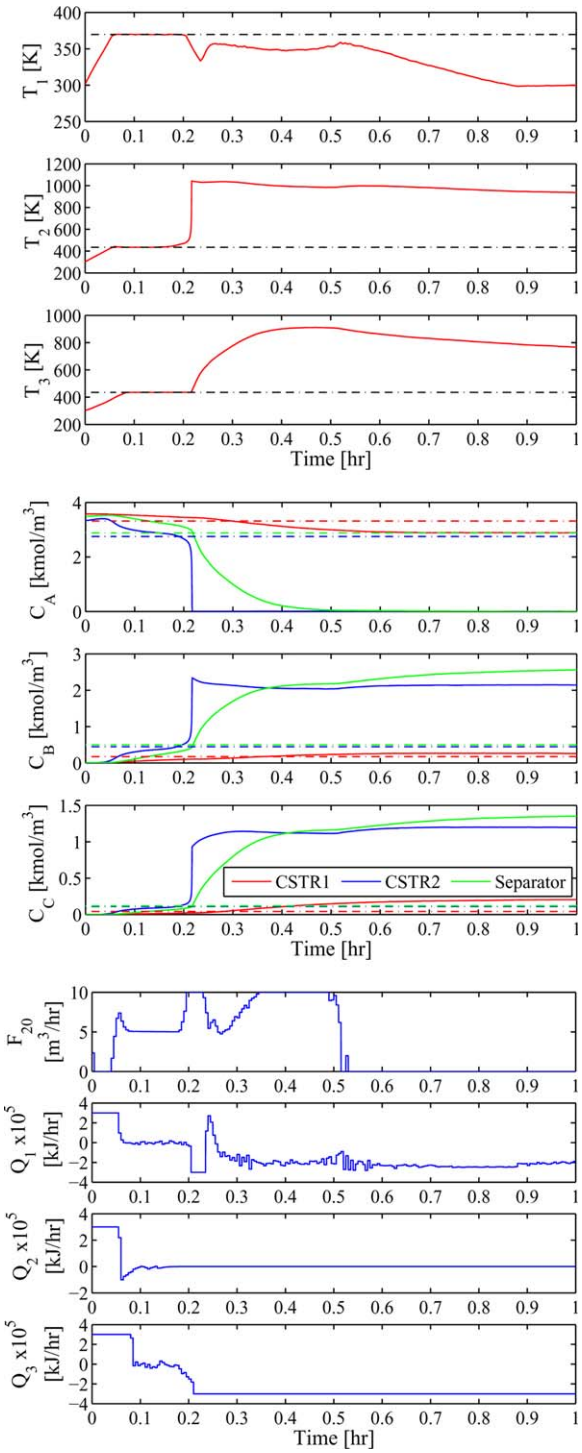

Figure 8. The closed-loop process state and manipulated input trajectories (solid lines) and set-points (dashed lines).

(a) vessel temperatures, (b) species concentrations, (c) manipulated inputs without proactive fault-tolerant control applied. The maximum available control energy in the faulty actuator of Q_2 follows the logistic function; the gradual fault starts at $t = 0.0545$ h. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

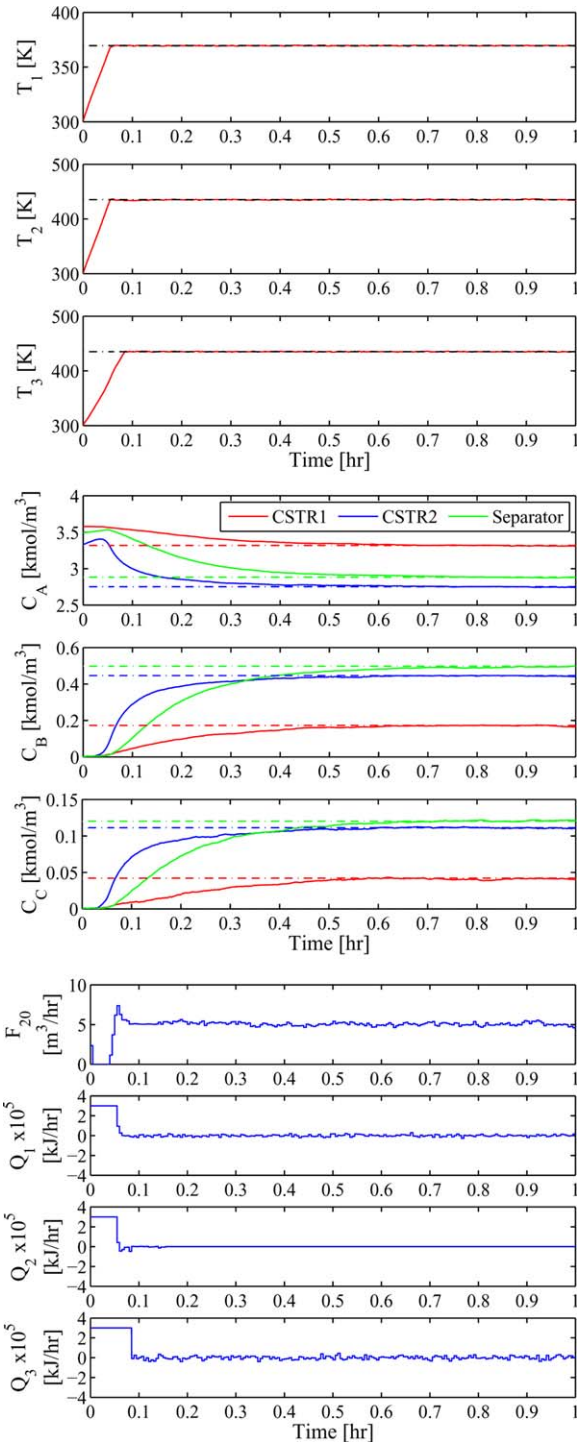

Figure 9. The closed-loop process state and manipulated input trajectories (solid lines) and set-points (dashed lines).

(a) vessel temperatures, (b) species concentrations, (c) manipulated inputs with proactive fault-tolerant control applied. The maximum available control energy in the faulty actuator of Q_2 follows the logistic function; the gradual fault starts at $t = 0.0545$ h. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

Specifically, by accounting for the gradual fault that limits the available maximum output of Q_2, the proactive fault-tolerant controller feeds less reactant material A into CSTR2 leading up to the fault and maintains the temperature T_2 at the desired steady-state as the maximum output of Q_2 decreases. The closed-loop process without proactive fault-tolerant control (Figure 3a) feeds more feedstock into

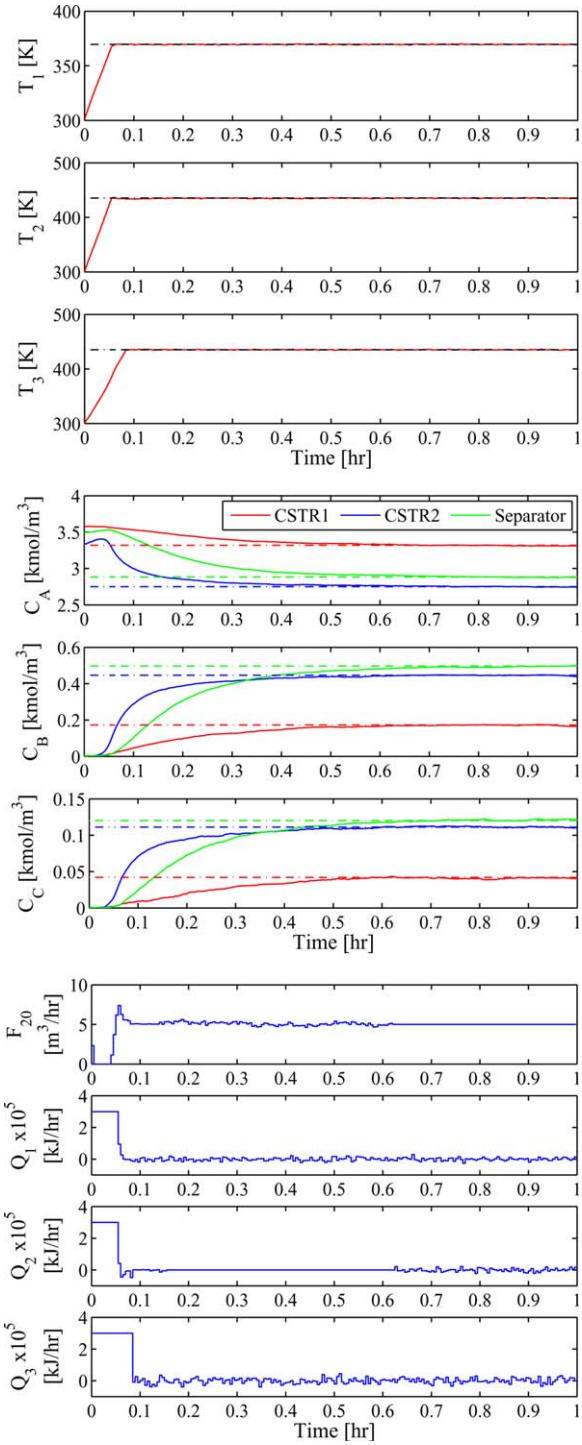

Figure 10. The closed-loop process state and manipulated input trajectories (solid lines) and set-points (dashed lines).

(a) vessel temperatures, (b) species concentrations and (c) manipulated inputs with the proposed proactive fault-tolerant LMPC. The maximum available control energy in the faulty actuator of Q_2 follows the logistic function with the given parameters. At $t = 0.625$h, the proactive fault-tolerant controller adds the repaired Q_2 actuator back to the closed-loop system. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

CSTR2 while demanding more heat removed to decrease the temperature T_2 to the desired steady-state after the fault. However, the fault has rendered the Q_2 actuator inactive and, therefore, cannot remove heat from CSTR2. The effect of feeding more material without removing heat causes the reactions to runaway because the reactions are highly exothermic. The post-fault behavior of these two control strategies is observed in Figures 8 and 9. The process under the proactive fault-tolerant controller brings the process states to the desired steady-state. The process without the proposed proactive LMPC settles on an offsetting steady-state. The total closed-loop performance index with the proposed proactive fault-tolerant LMPC is 2.55×10^4, which is an order of magnitude smaller than the closed-loop process with an LMPC that does not account for the fault which has a total closed-loop performance index of 3.76×10^5.

Process recovery from three input control system to fault-free four input control system

In this case, we demonstrate that with the proposed proactive LMPC we can successfully recover back to the full, fault-free system after an actuator fault has been rectified or replaced. Figure 10 shows the closed-loop evolution of the process with the proactive fault tolerant controller with the same gradual fault in the Q_2 actuator as in case study B. We consider $t = 0.625$h is the time the faulty actuator has been fixed and added back. From Figure 10, the controller is able to achieve practical stability both after the fault and after the faulty actuator has been fixed and added back to the system.

Conclusions

In this work, we proposed a proactive fault-tolerant Lyapunov-based MPC that can account for an incipient fault and work for complete fault rejection. We proved practical stability of a closed-loop nonlinear system with the proposed proactive fault-tolerant LMPC. The proposed controller was demonstrated through a chemical process consisting of two CSTRs in series followed by a flash separator. The simulated process demonstrated that the proactive fault-tolerant LMPC was able to achieve practical stability of the closed-loop system.

Acknowledgment

Financial support from the National Science Foundation is gratefully acknowledged.

Literature Cited

1. Christofides PD, Davis JF, El-Farra NH, Clark D, Harris KRD, Gipson JN. Smart plant operations: vision, progress and challenges. *AIChE J*. 2007;53:2734–2741.
2. Yuan Z, Zhang N, Chen B, Zhao J. Systematic controllability analysis for chemical processes. *AIChE J*. 2012;58:3096–3109.
3. Billinton R, Allan RN. Reliability evaluation of engineering systems: concepts and techniques. *Discrete Appl Math*. 1987;8:213–214.
4. Mhaskar P, Liu J, Christofides PD. *Fault-tolerant Process Control: Methods and Applications*. London, England: Springer-Verlag, 2013.
5. Zhang Y, Jiang J. Bibliographical review on reconfigurable fault-tolerant control systems. *Annu Rev Contr*. 2008;32:229–252.
6. Venkatasubramanian V, Rengaswamy R, Yin K, Kavuri SN. A review of process fault detection and diagnosis: Part I: Quantitative model-based methods. *Comput Chem Eng*. 2003;27:293–311.
7. Mhaskar P, Gani A, McFall C, Christofides PD, Davis JF. Fault-tolerant control of nonlinear process systems subject to sensor faults. *AIChE J*. 2007;53:654–668.
8. Mhaskar P, McFall C, Gani A, Christofides PD, Davis JF. Isolation and handling of actuator faults in nonlinear systems. *Automatica*. 2008;44:53–62.
9. Chilin D, Liu J, Chen X, Christofides PD. Fault detection and isolation and fault tolerant control of a catalytic alkylation of benzene process. *Chem Eng Sci*. 2012;78:155–166.
10. Bryner M. Smart manufacturing: the next revolution. *Chem Eng Prog*. 2012;108:4–12.
11. Bonfill A, Espua A, Puigjaner L. Proactive approach to address robust batch process scheduling under short-term uncertainties. *Comput Aided Chem Eng*. 2005;20:1057–1062.
12. Bonfill A, Espua A, Puigjaner L. Proactive approach to address the uncertainty in short-term scheduling. *Comput Chem Eng*. 2008;32:1689–1706.
13. Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery. *ACM Trans Comput Syst*. 2002;20:398–461.
14. Nagarajan AB, Mueller F, Engelmann C, Scott SL. Proactive fault tolerance for HPC with Xen virtualization. In: Proceedings of the 21st Annual International Conference on Supercomputing. New York, NY, Association for Computing Machinery (ACM), 2007:23–32.
15. Engelmann C, Valle G, Naughton T, Scott SL. Proactive fault tolerance using preemptive migration. In: *Proceedings of the 17th Euromicro International Conference on Parallel, Distributed and Network-Based Processing*. 18–20 Feb. 2009, Weimar, Germany, IEEE, 2009:252–257.
16. Yu J. A nonlinear kernel Gaussian mixture model based inferential monitoring approach for fault detection and diagnosis of chemical processes. *Chem Eng Sci*. 2012;68:506–519.
17. Rashid MM, Yu J. A new dissimilarity method integrating multidimensional mutual information and independent component analysis for non-Gaussian dynamic process monitoring. *Chemom Intell Lab Syst*. 2012;115:44–58.
18. Crowl DA, Louvar JF. *Chemical Process Safety: Fundamentals with Applications*. Upper Saddle River, NJ: Prentice Hall, 2001.
19. Salfner F, Malek M. Using hidden semi-Markov models for effective online failure prediction. In: *26th IEEE International Symposium on Reliable Distributed Systems*. 10–12 Oct. 2007, Beijing, China, IEEE, 2007:161–174.
20. Zhao Z, Wang F, Jia M, Wang S. Probabilistic fault prediction of incipient fault. In: *Chinese Control and Decision Conference (CCDC)*. 26–28 May 2010, Mianyang, China, IEEE, 2010:3911–3915.
21. Doymaz F, Romagnoli JA, Palazoglu A. A strategy for detection and isolation of sensor failures and process upsets. *Chemom Intell Lab Syst*. 2001;55:109–123.
22. Mhaskar P, El-Farra NH, Christofides PD. Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. *Syst Control Lett*. 2006;55:650–659.
23. Khalil HK. Nonlinear Systems. Upper Saddle River, NJ: Prentice Hall, 2002.
24. Massera JL. Contributions to stability theory. *Ann Math*. 1956;64:182–206.
25. Christofides PD, El-Farra NH. *Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-delays*. Berlin, Germany: Springer-Verlag, 2005.
26. Kokotović P, Arcak M. Constructive nonlinear control: a historical perspective. *Automatica*. 2001;37:637–662.
27. Lin Y, Sontag ED. A universal formula for stabilization with bounded controls. *Syst Control Lett*. 1990;16:393–397.
28. Muñoz de la Peña D, Christofides PD. Lyapunov-based model predictive control of nonlinear systems subject to data losses. *IEEE Trans Automat Contr*. 2008;53:2076–2089.
29. Wächter A, Biegler LT. On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. *Math Programming*. 2006;106:25–57.
30. Dummer GWA, Winton R, Tooley M. *An Elementary Guide to Reliability*. Butterworth-Heinemann, Boston, MA, 1997.
31. Von Seggern DH. *CRC Standard Curves and Surfaces with Mathematica*, *Vol. 1*. Boca Raton, FL: Chapman & Hall/CRC, 2006.

Manuscript received Nov. 6, 2012, and revision received Dec. 29, 2012.