2011 American Control Conference
on O'Farrell Street, San Francisco, CA, USA
June 29 - July 01, 2011

Data-Based Monitoring and Reconfiguration of a Distributed Model Predictive Control System

David Chilin, Jinfeng Liu, James F. Davis and Panagiotis D. Christofides

Abstract— **In this work, we develop a data-based monitoring and reconfiguration system for a distributed model predictive control system in the presence of control actuator faults. Specifically, we first design fault detection filters and filter residuals, which are computed via exponentially weighted moving average, to effectively detect faults. Then, we propose a fault isolation approach which uses adaptive fault isolation time windows to quickly and accurately isolate actuator faults. Simultaneously, we estimate the magnitudes of the faults using a least-squares method and based on the estimated fault values, we design appropriate fault-tolerant control strategies to handle the actuator faults and maintain the closed-loop system state within a desired operating region. A nonlinear chemical process example is used to demonstrate the approach.**

I. Introduction

In chemical process industry, there is a trend towards "smart" plants that are capable of highly automated control with decision making at the plant level taking into account environmental, health, safety and economic considerations [1], [2]. Along with the move towards more automated plant operation, improved methods of fault detection, isolation and handling are necessary due to the issues raised by automation itself. Fault tolerant control (FTC) is a field that has received a significant amount of attention recently in the context of process control and operations as a means for avoiding disaster in the case of a fault; see, for example [3], [4]. FTC attempts to reconfigure a process control system upon detection of a fault and isolation of its cause, in order to preserve closed-loop system stability and performance. Fault detection and isolation (FDI) methods can generally be divided into two categories: model-based and data-based. Model-based FDI methods generally rely on mathematical models of the process developed either from first principles or from system identification. With an accurate process model, it is possible to accomplish fault detection and isolation for specific process structures (see, for example, [5], [6]). Data-based methods, on the other hand, rely on process measurements in order to perform fault detection and isolation. While many of these methods have been successful in achieving fault detection, fault isolation remains a difficult task, particularly for nonlinear processes.

On the other hand, within process control, there is a trend towards distributed control architectures in which distributed optimization-based controllers compute the manipulated inputs in a coordinated fashion. Model predictive control (MPC) is a natural control framework to deal with the design of cooperative, distributed control systems because of its ability to handle input and state constraints, and also because it can compensate for the actions of other actuators. In recent literature, several distributed MPC (DMPC) methods have been proposed that deal with the coordination of separate MPCs that communicate in order to obtain optimal input trajectories in a distributed manner; see, for example, [7], [8], [9], [10]. In our previous work [11], we proposed a DMPC architecture with one-directional communication for nonlinear process systems. In this architecture, two separate MPCs designed via Lyapunov-based MPC (LMPC) were considered, in which one LMPC was used to guarantee the stability of the closed-loop system and the other LMPC was used to improve the closed-loop performance. In [12], we extended the DMPC architecture developed in [11] to include multiple distributed controllers and relaxed the requirement that one of the distributed controllers should be able to stabilize the closed-loop system. In [13], we developed an FDI and FTC system for the monitoring and reconfiguration of DMPC systems applied to general nonlinear processes in the presence of control actuator faults. The FDI and FTC system developed in [13] is based on process models and the assumption that once a faulty actuator is isolated, it can be reset to its zero state immediately.

In the present paper, we take advantage of both process models and process measurements to develop a monitoring and reconfiguration system for a distributed model predictive control (DMPC) system in the presence of control actuator faults. Specifically, we first design fault detection filters and corresponding filter residuals, which are computed via exponentially weighted moving average (EWMA), to effectively detect actuator faults. Then, we propose a fault isolation approach which uses adaptive fault isolation time windows to quickly and accurately isolate actuator faults. Simultaneously, we estimate the magnitudes of the faults using a least-squares method and based on the estimated fault values, we design appropriate fault-tolerant control (FTC) strategies to handle the actuator faults and maintain the closed-loop system state within a desired operating region. A nonlinear chemical process example is used to demonstrate the approach.

II. Notation

The operator $|\cdot|$ is used to denote the absolute value of a scalar and the operator $\|\cdot\|$ is used to denote Euclidean norm

David Chilin, Jinfeng Liu, James F. Davis and Panagiotis D. Christofides are with the Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA. Panagiotis D. Christofides is also with the Department of Electrical Engineering, University of California, Los Angeles, CA 90095-1592, USA. dchilin@ucla.edu, jinfeng@ucla.edu, jdavis@oit.ucla.edu and pdc@seas.ucla.edu.

978-1-4577-0079-8/11/$26.00 ©2011 AACC

of a vector, while $\|\cdot\|_Q$ refers to the square of a weighted Euclidean norm, defined by $\|x\|_Q = x^T Q x$ for all $x \in R^n$. The symbol $diag(v)$ denotes a square diagonal matrix whose diagonal elements are the elements of the vector v.

III. Problem formulation and preliminaries

A. Class of nonlinear systems

We consider nonlinear processes described by the following state-space model:

$$\dot{x}(t) = f(x) + \sum_{i=1}^{2} g_i(x)(u_i(t) + \tilde{u}_i(t)) \tag{1}$$

where $x \in R^n$ denotes the set of state variables, $u_1 \in R^{m_1}$ and $u_2 \in R^{m_2}$ denote two sets of manipulated inputs, $\tilde{u}_1 \in R^{m_1}$ and $\tilde{u}_2 \in R^{m_2}$ denote the unknown fault vectors for u_1 and u_2, respectively. We consider that $u_1 + \tilde{u}_1$ and $u_2 + \tilde{u}_2$ take values in non-empty convex sets $U_1 \in R^{m_1}$ and $U_2 \in R^{m_2}$, respectively. The convex sets U_1 and U_2 are defined as follows:

$$\begin{array}{rcl} U_1 & = & \{u_1 + \tilde{u}_1 \in R^{m_1} : \|u_1 + \tilde{u}_1\| \leq u_1^{\max}\} \\ U_2 & = & \{u_2 + \tilde{u}_2 \in R^{m_2} : \|u_2 + \tilde{u}_2\| \leq u_2^{\max}\} \end{array}$$

where $u_1^{\max}$ and $u_2^{\max}$ are the magnitudes of the input constraints. The system of Eq. 1 can be re-written in a compact form as follows:

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

where $g(x) = [g_1(x)\ g_2(x)]$, $u(t) = [u_1(t)^T\ u_2(t)^T]^T$ and $\tilde{u}(t) = [\tilde{u}_1(t)^T\ \tilde{u}_2(t)^T]^T$. We also assume that U is a suitable composition of U_1 and U_2 such that $u + \tilde{u} \in U$ is equivalent to $u_1 + \tilde{u}_1 \in U_1$ and $u_2 + \tilde{u}_2 \in U_2$.

We use the variable $\tilde{u}_{f,j}$, $j = 1, \ldots, m_1 + m_2$, to model the possible faults associated with the j^{th} element in the manipulated input vector u. Under fault-free operating conditions, we have $\tilde{u} = 0$, and hence, $\tilde{u}_{f,j} = 0$ for all $j = 1, \ldots, m_1 + m_2$. When fault j occurs, $\tilde{u}_{f,j}$ takes a non-zero value. We assume that f and g are locally Lipschitz vector functions and that $f(0) = 0$. This means that the origin is an equilibrium point for the fault-free system ($\tilde{u} = 0$ for all t) with $u = 0$. We also assume that the state x of the system is available synchronously and continuously.

B. Fault-free control system design

We assume that there exists a nonlinear control law $h(x)$ which determines u_1 (i.e., $u_1(t) = h(x(t))$) and renders the origin of the fault-free closed-loop system asymptotically stable with $u_2(t) = 0$. This assumption is essentially a standard stabilizability requirement made in all linear/nonlinear control methods and implies that there exists a Lyapunov function $V(x)$ of the system whose time derivative is always negative when $u_1 = h(x)$ is applied to the fault-free closed-loop system [14], [15].

We adopt the DMPC architecture introduced in [11] to design the fault-free control system. In this DMPC architecture, one LMPC is designed to determine u_1 and is responsible for the closed-loop stability; another LMPC is designed to compute u_2 and to coordinate with u_1 to improve the closed-loop performance. We will refer to the two LMPCs computing u_1 and u_2 as LMPC 1 and LMPC 2, respectively. The two LMPCs are evaluated in a sequential fashion (i.e., LMPC 2 is first evaluated and then LMPC 1 is evaluated) at discrete time instants $\{t_{k\geq 0}\}$ with $t_k = t_0 + k\Delta,\ k = 0, 1, \ldots$ where t_0 is the initial time and Δ is a sampling time.

Specifically, the optimization problem of LMPC 2 at time t_k depends on the state measurement $x(t_k)$ and is formulated as follows:

$$\min_{u_2 \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(\tau), u_1(\tau), u_2(\tau)) d\tau \tag{2a}$$

$$\dot{\tilde{x}}(t) = f(\tilde{x}(t)) + \sum_{i=1}^{2} g_i(\tilde{x}(t)) u_i(t),\ \tilde{x}(t_k) = x(t_k) \tag{2b}$$

$$u_1(t) = h(\tilde{x}(t_{k+j})), \forall\, t \in [t_{k+j}, t_{k+j+1}), u_2(t) \in U_2 \tag{2c}$$

$$\frac{\partial V(x)}{\partial x} g_2(x(t_k)) u_2(t_k) \leq 0 \tag{2d}$$

with $L(\tilde{x}, u_1, u_2) = \|\tilde{x}(\tau)\|_{Q_c} + \|u_1(\tau)\|_{R_{c1}} + \|u_2(\tau)\|_{R_{c2}}$ where $S(\Delta)$ is the family of piece-wise constant functions with sampling period Δ, N is the prediction horizon, Q_c, R_{c1} and R_{c2} are positive definite weighting matrices, $j = 0, \ldots, N-1$, $\tilde{x}$ is the predicted trajectory of the fault-free system with u_2 being the input trajectory computed by LMPC 2 of Eq. 2 and u_1 being the nonlinear controller $h(x)$ applied in a sample-and-hold fashion. The optimal solution to this optimization problem is denoted $u_2^*(t|t_k)$. This information is sent to LMPC 1. The optimization problem of LMPC 1 depends on $x(t_k)$ and the decision made by LMPC 2 (i.e., $u_2^*(t|t_k)$). Specifically, LMPC 1 is based on the following optimization problem:

$$\min_{u_1 \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(\tau), u_1(\tau), u_2(\tau)) d\tau \tag{3a}$$

$$\dot{\tilde{x}}(t) = f(\tilde{x}(t)) + \sum_{i=1}^{2} g_i(\tilde{x}(t)) u_i(t),\ \tilde{x}(t_k) = x(t_k) \tag{3b}$$

$$u_1(t) \in U_1,\ u_2(t) = u_2^*(t|t_k) \tag{3c}$$

$$\frac{\partial V(x)}{\partial x} g_1(x(t_k)) u_1(t_k) \leq \frac{\partial V(x)}{\partial x} g_1(x(t_k)) h(x(t_k)). \tag{3d}$$

The optimal solution to this optimization problem is denoted by $u_1^*(t|t_k)$.

Once both optimization problems are solved, the manipulated inputs of the DMPC system based on LMPC 1 and LMPC 2 are defined as follows:

$$u_1^L(t) \;=\; u_1^*(t|t_k),\ u_2^L(t) = u_2^*(t|t_k),\ \forall t \in [t_k, t_{k+1}).$$

The fault-free closed-loop system of Eq. 1 under this DMPC scheme with inputs defined by $u_1 = u_1^L$ and $u_2 = u_2^L$ maintains practical stability because of the two Lyapunov-based constraints of Eqs. 2d and 3d [11].

C. FTC considerations

The presence of the control action u_2 brings extra control flexibility to the closed-loop system which can be used to carry out FTC. Specifically, we further assume that the control input u_1 can be decomposed into two subsets (i.e.,

$u_1 = [u_{11}^T\ u_{12}^T]^T$) and that there exists a nonlinear control law $h_2(x) = [h_{21}(x)^T\ h_{22}(x)^T]^T$ which determines u_{11} and u_2 (i.e., $u_{11} = h_{21}(x)$ and $u_2 = h_{22}(x)$) and is able to asymptotically stabilize the fault-free closed-loop system with $u_{12} = 0$. This assumption implies that there exist a Lyapunov function $V_2(x)$ of the system whose time derivative is always negative when $u_{11} = h_{21}(x)$, $u_{12} = 0$ and $u_2 = h_{22}(x)$ are applied.

Based on $h_2(x)$, we can design a backup DMPC system to manipulate u_{11} and u_2 to stabilize the closed-loop system following the results developed in [12]. We still design two LMPC controllers in the backup DMPC system. One LMPC is used to manipulate u_{11} and the other one is used to manipulate u_2. In this backup DMPC system, the two LMPCs coordinate their actions to maintain the closed-loop stability. We refer to the LMPC manipulating u_{11} as the backup LMPC 1 and the LMPC manipulating u_2 as the backup LMPC 2. The two backup LMPCs are also evaluated in sequence.

The backup LMPC 2 optimizes u_2 and is designed as follows:

$$\min_{u_2 \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(\tau), u_1(\tau), u_2(\tau))d\tau \tag{4a}$$

$$\begin{aligned} \dot{\tilde{x}}(t) = f(\tilde{x}(t)) + g_1(\tilde{x}(t))[u_{11}(t)^T u_{12}(t)^T]^T \\ + g_2(\tilde{x}(t))u_2(t),\ \tilde{x}(t_k) = x(t_k) \end{aligned} \tag{4b}$$

$$u_{11}(t) = h_{21}(\tilde{x}(t_{k+j})),\ \forall\, t \in [t_{k+j}, t_{k+j+1}) \tag{4c}$$

$$u_{12}(t) = 0,\ u_2(t) \in U_2 \tag{4d}$$

$$\frac{\partial V_2(x)}{\partial x} g_2(x(t_k))u_2(t_k) \leq \frac{\partial V_2(x)}{\partial x} g_2(x(t_k))h_{22}(x(t_k)). \tag{4e}$$

The solution to the optimization problem of Eq. 4 is denoted $u_2^{b,*}(t|t_k)$. The backup LMPC 1 optimizes u_{11} and is designed as follows:

$$\min_{u_{11} \in S(\Delta)} \int_{t_k}^{t_{k+N}} L(\tilde{x}(\tau), u_1(\tau), u_2(\tau))d\tau \tag{5a}$$

$$\begin{aligned} \dot{\tilde{x}}(t) = f(\tilde{x}(t)) + g_1(\tilde{x}(t))[u_{11}(t)^T u12(t)^T]^T \\ + g_2(\tilde{x}(t))u_2(t),\ \tilde{x}(t_k) = x(t_k) \end{aligned} \tag{5b}$$

$$u_{11}(t) \in U_1,\ u_{12}(t) = 0,\ u_2 = u_2^{b,*}(t|t_k) \tag{5c}$$

$$\begin{aligned} &\frac{\partial V_2(x)}{\partial x} g_1(x(t_k))[u_{11}(t)^T\ 0^T]^T \\ &\quad \leq \frac{\partial V_2(x)}{\partial x} g_1(x(t_k))[h_{21}(x(t_k))^T\ 0^T]^T. \end{aligned} \tag{5d}$$

The solution to the optimization problem of Eq. 5 is denoted $u_{11}^{b,*}(t|t_k)$. The control inputs of the backup DMPC are defined as follows:

$$\begin{aligned} &u_{11}^b(t) = u_{11}^{b,*}(t|t_k),\ u_2^b(t) = u_2^{b,*}(t|t_k),\ \forall t \in [t_k, t_{k+1}) \\ &u_{12}^b(t) = 0,\ \forall t \end{aligned}$$

The fault-free closed-loop system of Eq. 1 under the backup DMPC control with inputs defined by $u_{11} = u_{11}^b$, $u_{12} = 0$ and $u_2 = u_2^b$ maintains practical stability of the closed-loop system because of the Lyapunov-based constraints of Eqs. 4e and 5d [12].

To present the proposed method, in this work, we consider control actuator faults that can be detected by appropriate nonlinear dynamic fault filters via observing the evolution of the closed-loop system state. In order to isolate the occurrence of a fault, it is further required to assume that the control actuator in question is the only one influencing the observed "faulty" states (i.e., each fault has a unique fault signature). For more discussions on systems having verifiable isolable structures, please see [6], [16].

IV. FDI AND FTC SYSTEM DESIGN

In this section, we develop a combined model-based and data-based FDI and FTC method for the closed-loop system of Eq. 1 under the DMPC of Eqs. 2-3.

A. Design of fault detection filters and residuals

The DMPC system of Eqs. 2-3 is the control configuration for the fault-free system of Eq. 1. We first design an FDI scheme to detect faults in this control system. In this FDI scheme, a filter is designed for each state and the design of the filter for the p^{th}, $p = 1, \ldots, n$, state in the system state vector x is as follows [6]:

$$\dot{\hat{x}}_p(t) = f_p(X_p) + g_{1p}(X_p)u_1^L(t) + g_{2p}(X_p)u_2^L(t) \tag{6}$$

where $\hat{x}_p$ is the filter output for the p^{th} state, f_p, g_{1p} and g_{2p} are the p^{th} components of the vector functions f, g_1 and g_2, respectively. The state X_p is obtained from both the actual state measurements, x, and the filter output, $\hat{x}_p$, as follows:

$$X_p(t) = [x_1(t), \ldots, x_{p-1}(t), \hat{x}_p(t), x_{p+1}(t), \ldots, x_n(t)]^T.$$

Note that in the filter of Eq. 6, the control inputs $u_1^L(t)$ and $u_2^L(t)$ are determined by LMPC 1 of Eq. 3 and LMPC 2 of Eq. 2 as applied to the actual process based on the state X_p, and are updated every control sampling time Δ (i.e., the sampling time instants $\{t_{k\geq 0}\}$).

The FDI filters are only initialized at $t = 0$ such that $\hat{x}_p(0) = x_p(0)$. The information generated by the filters provides a fault-free estimate of the actual system state at any time t and allows easy detection of the actual system state deviations due to faults. For each state associated with a filter, an FDI residual is defined as follows:

$$r_p(t) = \|\hat{x}_p(t) - x_p(t)\|$$

with $p = 1, \ldots, n$. The residual r_p is computed continuously because $\hat{x}_p(t)$ is known for all t and the state measurement, x, is also available for all t. If no fault occurs, the filter states track the system states. In this case, the dynamics of the system states and the FDI filter states are identical, so $r_p(t) = 0$ for all times.

In the practical case where sensor measurement noise and process noise are present, the residual will be nonzero even without an actuator fault. In order to reduce the influence of process noise on fault detection, we define a weighted residual $r_{E,p}, p = 1, ..., n$, for each residual r_p, calculated at discrete time instants $\{t_{i\geq 0}\}$ with $t_i = t_0 + i\Delta_r, i = 0, 1, 2, ...$ The weighted residual is calculated using an exponentially weighted moving average (EWMA) method as follows [17]:

$$r_{E,p}(t_i) = \lambda r_p(t_i) + (1-\lambda) r_{E,p}(t_{i-1}) \tag{7}$$

with $r_{E,p}(t_0) = r_p(t_0)$ and the weighting factor $\lambda \in (0,1]$. The parameter λ determines the rate at which previous data enter into the calculations of the weighted residual. When $\lambda = 1, r_{E,p}$ is equivalent to r_p. The benefit of using EWMA residuals is their ability to better capture smaller drifts in the system and protection against occasional spikes. The value of λ is typically set between 0.2 and 0.5 depending on the sensitivity and responsiveness desired [17]. All further mention of residuals will be in reference to the EWMA residuals.

Also due to sensor measurement and process noise, fault detection thresholds are necessary so that a fault is declared only when a residual exceeds its specific threshold value. The thresholds are based on historical process variance data under no fault (normal) operating conditions and chosen to the desired degree of confidence to quickly detect possible faults. In some cases, the residual may deviate temporarily due to normal process variance and should not be interpreted as a fault. In these cases, it is important to properly confirm that the residual is deviating because of a fault by waiting a specified amount of time. This waiting time gives a certain degree of confidence that a fault has occurred and reduces the incidence of false alarms. In the detection of a fault, three threshold values for each EWMA residual are used. The threshold values for $r_{E,p}$ are calculated as follows [17]:

$$\sigma_{p,k} = \bar{r}_p + k s_p \sqrt{\frac{\lambda}{2-\lambda}} \tag{8}$$

where $k = 3, 4, 5$ is a weighting factor, $\bar{r}_p$ and s_p are the mean value and standard deviation of the p^{th} residual (r_p) based on historical fault-free operation data, respectively. In the remainder, we will refer to the threshold values of a residual with $k = 3$, $k = 4$ and $k = 5$ as the first, the second and the third threshold of the residual, respectively.

B. Fault detection and isolation using adaptive windows

In this subsection, we augment our previous FDI system [6] to include an adjustable time window based on the rate of change of the residual with the goals of reducing the probability of false alarms, false isolation and achieving a quicker fault recovery response.

On the occurrence of a fault, certain residuals directly associated with the fault will immediately become nonzero at different rates (or in the case where process noise and measurement noise are present their thresholds will be exceeded at different times depending on the fault's magnitude). An improvement over previous work is the use of EWMA residuals in combination with adjustable fault isolation time windows.

When there is a residual that exceeds its second threshold and stays above it for a time period Δt_d, then a fault is declared. For example, if $r_{E,p}$ exceeds $\sigma_{p,4}$ at time $t_{\sigma_{p,4}}$ and stays above $\sigma_{p,4}$ from $t_{\sigma_{p,4}}$ to $t_{\sigma_{p,4}} + \Delta t_d$, then a fault is declared. The waiting time Δt_d is used to reduce the incidence of false alarms, in particular, intermittent spikes.

Fault isolation is carried out simultaneously with fault detection. Based on the rate of change of the first residual which exceeds its second threshold, a time window over which a fault may be isolated is calculated. If there is no residual that goes up and exceeds its third threshold within the time window, the fault is isolated at the end of the time window. The isolated fault has a signature composed of all the residuals that exceed their second threshold. If there is at least residual that exceeds its third threshold within the fault isolation time window, the fault is isolated at the time the first residual exceeding its third threshold. For example, if $r_{E,p}$ is the first residual that exceeds its threshold $\sigma_{p,4}$, a time window, Δt_p, is calculated as follows:

$$\Delta t_p = w(t_{\sigma_{p,4}} - t_{\sigma_{p,3}}) \tag{9}$$

where w is a constant or a complex function of the model and its current state, and $t_{\sigma_{p,4}}$ and $t_{\sigma_{p,3}}$ are the time instants the residual $r_{E,p}$ exceeds $\sigma_{p,4}$ and $\sigma_{p,3}$, respectively. If from $t_{\sigma_{p,4}}$ to $t_{\sigma_{p,4}} + \Delta t_p$, there is no residual that exceeds its third threshold, the fault is isolated at time $t_{\sigma_{p,4}} + \Delta t_p$ with a signature composed of all the residuals whose values exceed their second thresholds. If from $t_{\sigma_{p,4}}$ to $t_{\sigma_{p,4}} + \Delta t_p$, there is at least one residual that exceed its third threshold, for example, $r_{E,q}$ exceeds $\sigma_{q,5}$ at time $t_{\sigma_{q,5}}$, then the fault is isolated at $t_{\sigma_{q,5}}$.

C. Fault parameter estimation

After a fault has been isolated, the FTC system must know the magnitude of the fault in order to target the corresponding new operating point and properly stabilize the system in the presence of the fault. To simplify the description of the proposed method, we consider faults of constant magnitudes in this work; however, faults with time-varying values can be handled using the proposed method in a straightforward manner.

When a residual ($r_{E,p}$) exceeds its first threshold ($\sigma_{p,3}$), we begin to collect the sampled system states as well as the actual control inputs applied to the system. When the fault is confirmed and isolated, a least square optimization problem is solved to get an estimate of the magnitude of the fault based on the collected sampled system states and the actual control inputs. Specifically, we collect the sampled system states, $x(t)$, and record the actual control inputs (i.e., $u_1(t) = u_1^L(t)$ and $u_2(t) = u_2^L(t)$) applied to the system for $t_{\sigma_{p,3}}$ to the fault isolation time $t_{isolate}$ with a sampling time Δ_e. The magnitude of the fault $\tilde{u}_{f,j}$ is estimated by solving the following optimization problem:

$$\min_{\tilde{u}_{f,j}} \sum_{i=0}^{M} \left(x(t_f + i\Delta_e) - \tilde{x}(t_f + i\Delta_e) \right)^2 \tag{10a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t)) + g(\tilde{x}(t))(u^L(t) + d) \tag{10b}$$

$$\tilde{x}(t_f) = x(t_f) \tag{10c}$$

where $u^L(t) = [u_1^L(t)^T \; u_2^L(t)^T]^T$ is the actual control inputs that have been applied to the closed-loop system from $t_{\sigma_{p,3}}$

to $t_{isolate}$, M is the maximum integer satisfying $M\Delta_e \leq t_{isolate} - t_{\sigma_{p,3}}$, $d = [0 \ \cdots \ \tilde{u}_{f,j} \ \cdots \ 0]^T$ is the fault vector, and $x(t_f)$ is the system state at the fault detection time. The solution to the optimization problem of Eq. 10 is denoted $\tilde{u}^*_{f,j}$, which is an optimal estimate of the actual fault $\tilde{u}_{f,j}$ from a least-square point of view.

D. FTC strategies

When a fault is detected, isolated and the magnitude of the fault is estimated, suitable FTC strategies can be carried out to keep the closed-loop system state within a desired operating region. Because of the faults, the origin (the operating point of the fault-free system) may be not achievable because of the input constraints and the system structure. In this case, we may operate the system at a new operating point within the desired operating region. To determine the new operating point x_s, we propose to solve an optimization problem. Specifically, when the fault is $\tilde{u}^*_{f,j}$, the new operating point, x_s, is obtained by solving the following optimization problem:

$$\min_{x_s, u_s} \|x_s\|_S \tag{11a}$$

$$\text{s.t. } f(x_s) + g(x_s)(u_s + d) = 0 \tag{11b}$$

$$u_s + d \in U \tag{11c}$$

$$x_s \in X \tag{11d}$$

where S is a positive weighting matrix, $d = [0 \ \cdots \ \tilde{u}^*_{f,j} \ \cdots \ 0]^T$ and X denotes the desired operating state region. The objective of the above optimization problem is to find an operating point within the desired operating state region such that the distance (measured by weighted Euclidean norm) between the new operating point and the origin is minimized. We assume that the optimization problem of Eq. 11 is always feasible which implies that we can always find the new operating point x_s and the corresponding new steady-state control input values $u_s = [u_{1s}^T \ u_{2s}^T]^T$.

Note that the proposed method is only one of many possible approaches to determine the new operating point in the case of a fault. The basic idea of the proposed method is to find a new operating point that stays as close as possible to the original operating point (i.e., the origin $x = 0$).

Once we find the new operating point x_s, we proceed to design the FTC strategies for the fault-free DMPC system (see Eqs. 2-3) in the presence of actuator faults. In general, when there is a fault in the control system, it is impossible to carry out FTC unless there is another backup control loop. However, in the fault-free DMPC system, because of the extra control flexibility brought into the whole system by u_2 (LMPC 2), it is possible in some cases to carry out FTC without activating new control actuators.

When there is a persistent fault in the loop of u_2 which is denoted d_2, and the fault can be detected and isolated in a reasonable time frame, it is possible to switch off the controller LMPC 2 and only use u_1 in the control system. When LMPC 2 is switched off from the closed-loop system, u_2 is set by the fault (i.e., $u_2 = d_2$); and in the DMPC scheme of Eqs. 2-3, only LMPC 1 is evaluated each sampling time. In order to maintain the stability of the closed-loop system, the design of LMPC 1 will need to be updated with the new operating point and its corresponding new steady-state control input values (i.e., the cost function $L(x, u_1, u_2)$ needs to be updated with x_s and u_s in a way such that $L(x_s, u_{1s}, u_{2s}) = 0$), and updated with the fault magnitude information (i.e., $u_2 = d_2$); the design of $h(x)$ also needs to be updated with the new steady-state information. The control inputs determined by the updated LMPC 1 will be referred to as $u_1'(x)$.

This FTC strategy will maintain the closed-loop stability if implemented quickly such that the state of the system is still within the stability region of the backup controllers and parameter estimation is sufficiently accurate, however, the performance of the closed-loop system may degrade to some extent.

When there is a fault in the subset u_{12} which is denoted d_1, the FTC strategy would shut down the control action of u_{12} and reconfigure the DMPC algorithms to the backup DMPC of Eqs. 4-5 to manipulate u_{11} and u_2 to control the process. In order to maintain the stability of the closed-loop system, the designs of the two backup LMPCs and the design of $h_2(x)$ needs to be updated with the new operating point and corresponding new steady-state control input values; as well as being updated with the fault magnitude information. The control inputs determined by the updated designs will be referred to as $u_1''(x)$ and $u_2''(x)$.

However, when there is a fault in the subset u_{11}, it is impossible to successfully carry out FTC without activating backup actuators within the DMPC systems for the class of nonlinear systems considered in this work.

The FTC switching rules for the system of Eq. 1 within the DMPC system of Eqs. 2-3 are described as follows:

1) When a fault in the actuator associated with u_2 is isolated at t_f, the FTC switching rule is:

$$u_1(t) = \begin{cases} u_1^L(x), & t \leq t_f \\ u_1', & t > t_f \end{cases} \tag{12a}$$

$$u_2(t) = \begin{cases} u_2^L(x), & t \leq t_f \\ d_2, & t > t_f \end{cases} \tag{12b}$$

2) When a fault in the actuator associated with u_{12} is detected at t_f, the FTC switching rule is:

$$u_1(t) = \begin{cases} u_1^L(x), & t \leq t_f \\ \begin{bmatrix} u_{11}''(x) \\ d_1 \end{bmatrix}, & t > t_f \end{cases} \tag{13a}$$

$$u_2(t) = \begin{cases} u_2^L(x), & t \leq t_f \\ u_2''(x), & t > t_f \end{cases} \tag{13b}$$

V. Application to a reactor-separator process

A. Process description and modeling

The process considered in this study is a three vessel, reactor-separator system consisting of two CSTRs and a flash tank separator as shown in Fig. 1. Its detailed description and modeling can be found in [13]. Sensor and process noise

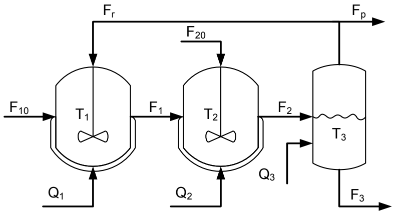

Fig. 1. Two CSTRs and a flash tank with recycle stream.

TABLE I

THE DESIRED OPERATING STEADY-STATE x_s.

T_1	C_{A1}	C_{B1}	C_{C1}
370 $[K]$	3.32 $[kmol/m^3]$	0.17 $[kmol/m^3]$	0.04 $[kmol/m^3]$
T_2	C_{A2}	C_{B2}	C_{C2}
435 $[K]$	2.75 $[kmol/m^3]$	0.45 $[kmol/m^3]$	0.11 $[kmol/m^3]$
T_3	C_{A3}	C_{B3}	C_{C3}
435 $[K]$	2.88 $[kmol/m^3]$	0.50 $[kmol/m^3]$	0.12 $[kmol/m^3]$

were added to the simulations. The desired operating steady-state is the unstable steady state, x_s, whose values are shown in Table I.

For this process, we have two sets of manipulated inputs. The first set of manipulated inputs is the heat injected to or removed from the three vessels, that is $u_1 = [Q_1 - Q_{1s}\ Q_2 - Q_{2s}\ Q_3 - Q_{3s}]^T$; the second set includes the inlet flow rate to vessel 2, that is $u_2 = F_{20} - F_{20s}$. The variables Q_{1s}, Q_{2s}, Q_3s and F_{20s} denote the steady-state input values of the inputs whose values are shown in Table II. The control inputs are subject to the constraints $|Q_i - Q_{is}| \leq u_1^{\max} = 10^6\ KJ/hr, (i = 1, 2, 3)$ and $|F_{20} - F_{20s}| \leq u_2^{\max} = 5\ m^3/hr$.

In the design of the fault free DMPC system for the process, we consider a quadratic Lyapunov function $V(x) = x^T Px$ with $P = diag([20\ 10^3\ 10^3\ 10^3\ 10\ 10^3\ 10^3\ 10^3\ 10\ 10^3\ 10^3\ 10^3])$ and design the controller $h(x)$ as three PI controllers with proportional gains $K_{p1} = K_{p2} = K_{p3} = 8000$ and integral time constants $\tau_{I1} = \tau_{I2} = \tau_{I3} = 10$ based on the measurements of T_1, T_2 and T_3, respectively. Note that, in the absence of process noise and measurement noise, this design of $h(x)$ manipulating u_1 can stabilize the closed-loop system asymptotically without the use of u_2. Based on $h(x)$ and $V(x)$, we design LMPC 1 following Eq. 3 to determine u_1 and LMPC 2 following Eq. 2 to determine u_2. In the design of the LMPCs, the weighting matrices are chosen to be $Q_c = P$, $R_1 = diag([(5\ 5\ 5) \cdot 10^{-12}])$ and $R_2 = 100$. The horizon for the optimization problem is $N = 4$ with a time step of $\Delta = 0.05\ hr$.

In addition, the set of control inputs u_1 can be divided into two subsets, $u_{11} = [Q_1 - Q_{1s}\ Q_3 - Q_{3s}]^T$ and $u_{12} = Q_2 - Q_{2s}$. The input combination u_{11} and u_2 is able to stabilize the closed-loop system which can be used as the input configuration of the backup DMPC system of Eqs. 4-5. In order to design the backup DMPC, we need to design a second Lyapunov-based controller $h_2(x)$ which manipulates u_{11} and u_2. We also design h_2 through PI control law with proportional gains $K^b_{p1} = K^b_{p2} = 8000$, $K^b_{p3} = -0.3$ and integral time constants $\tau^b_{I1} = \tau^b_{I2} = \tau^b_{I3} = 10$ based on the measurements of T_1, T_3 and T_2, respectively. The control design h_2 can stabilize the closed-loop system asymptotically with $Q_2 = 0$ in the absence of process noise and measurement noise. In the design of the backup DMPC system, we choose $V_2(x) = V(x)$.

TABLE II

THE STEADY-STATE INPUT VALUES.

Q_{1s}	Q_{2s}	Q_{3s}	F_{20s}
0 $[KJ/hr]$	0 $[KJ/hr]$	0 $[KJ/hr]$	5 $[m^3/hr]$

TABLE III

EWMA RESIDUAL MEANS AND STANDARD DEVIATION.

$\bar{r}_{T_2}$	$\bar{r}_{CA2}$	$\bar{r}_{CB2}$	$\bar{r}_{CC2}$
0.664900	0.013944	0.003421	0.003980
s_{T_2}	s_{CA2}	s_{CB2}	s_{CC2}
0.464139	0.010351	0.002810	0.002960

In order to perform FDI for the reactor-separator system, we construct the FDI filters for the states affected directly by the four manipulated inputs as in Eq. 6. The states affected directly by the manipulated inputs are T_1, C_{A2}, C_{B2}, C_{C2}, T_2 and T_3. The FDI residuals take the following form:

$$\begin{array}{rcl} r_{T_i}(t) & = & |\hat{T}_i(t) - T_i(t)|, \quad i = 1, 2, 3 \\ r_{C_{i2}}(t) & = & |\hat{C}_{i2}(t) - C_{i2}(t)|, \quad i = A, B, C. \end{array} \tag{14}$$

Based on these residuals, we design the EWMA residuals with $\lambda = 0.5$ and the sampling time $\Delta_r = 0.005$. The mean values and standard deviations of the EWMA residuals are shown in Table III.

We consider two different faults in the following simulations. First, we consider a fault in the heat input/removal actuator to vessel 2, that is a fault in Q_2. Because Q_2 only affects the state T_2 directly and all the measurements are continuously available, when there is an actuator fault in Q_2, only the residual corresponding to T_2 exceeds its threshold. The second fault we consider is a fault in the inlet flow actuator to vessel 2, that is a fault in F_{20}. Because the control action F_{20} affects directly the states T_2, C_{A2}, C_{B2} and C_{C2}, when there is an actuator fault in F_{20}, more than one residuals will exceed their thresholds. In the simulations, $\Delta t_d = 36\ s$, $w = 3$ and $\Delta_e = 0.005\ hr$.

B. Simulation Results

Three different simulation sets are presented to show the merits of isolating using the adaptive windows based on EWMA residuals. For each simulation, the plant is initialized at the desired steady-state x_s (see Table I) and simulated to $5.0\ hr$ with a fault being triggered at $1.050hr$.

In the first set of simulations, a Q_2 fault with a magnitude of 20% of $u_1^{\max}$ is triggered at $1.050\ hr$ (we will refer to it as "small" Q_2 fault). From the design of the system, the Q_2 fault directly affects the temperature in vessel 2 where the residual for T_2 begins to deviate. When the residual for T_2, r_{E,T_2}, (see top left plot of Fig. 2) exceeds a chosen confidence level (i.e., its first threshold $\sigma_{T_2,3}$) at $1.065\ hr$, the FDI system begins monitoring the rates of change of all the residuals. The residual r_{E,T_2} is the first to exceed its second

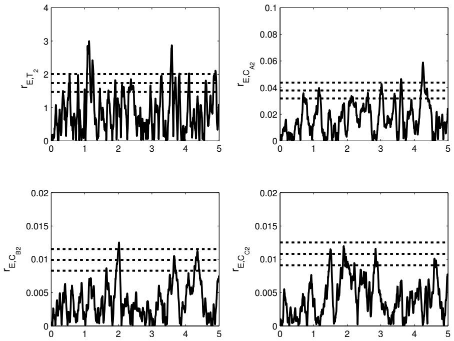

Fig. 2. Case 1: Q_2 "small" fault is isolated using longer waiting time based on slow residual change of T_2. The dotted lines correspond to the 1^{st}, 2^{nd},and 3^{rd} residual threshold, and the solid line correspond to EWMA residual. The residual r_{E,T_2} exceeds $\sigma_{T_2,3}$ at 1.065 hr and $\sigma_{T_2,4}$ at 1.070 hr where an fault isolation window is set to 3.6 min. The residual r_{E,T_2} exceeds $\sigma_{T_2,5}$ at 1.075 hr and the fault is isolated at 1.085 hr. The fault is estimated as 18.5 KJ/hr (actual 20 KJ/hr).

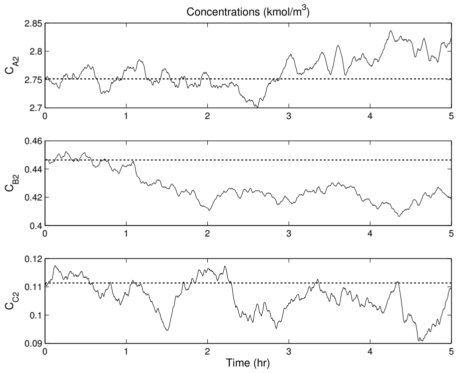

Fig. 3. Case 1: Q_2 "small" fault is isolated and control system is reconfigured to stabilize the closed-loop system - Concentrations.

threshold $\sigma_{T_2,4}$ at 1.070 hr. At time 1.075 hr, the FDI system also calculates a time window of 0.05 $hr = 3.6$ min to insure proper isolation of the fault. However, because r_{E,T_2} deviates quickly and exceeds $\sigma_{T_2,5}$ at 1.075 hr, the fault is isolated at 1.085 hr after waiting for 0.01 hr to confirm it. The fault is also isolated at 1.085 hr with a fault estimate of 18.5 KJ/hr (actual fault value is 20 KJ/hr). The fault tolerant control system reconfigures and is able to stabilizes the system near the target steady state by 1.500 hr as shown in the concentration profiles in Fig. 3 and the temperature profiles in Fig. 4.

In case 2, a Q_2 fault set to a magnitude of 99% of $u_1^{\max}$ is triggered at 1.050 hr (we will refer to it as "large" Q_2 fault). The larger Q_2 fault will demonstrate the FDI's quicker response and improved robustness when used in conjunction with fault tolerant control. In Fig. 5, the "large" fault compared to a "small" fault of case 1 (Fig. 2) causes the residual to deviate much quicker with the FDI beginning to monitor at 1.060 hr with a calculated isolation window of 36 s. The fault is isolated early at 1.070 hr soon after the r_{E,T_2} exceeded $\sigma_{T_2,5}$, and the fault is estimated to be 100 KJ/hr (actual 99 KJ/hr). Figures 6 and 7 show that the FTC system is able to stabilize the system at a new steady-state after reconfiguration at 1.080 hr.

The purpose of the third case is to better illustrate the

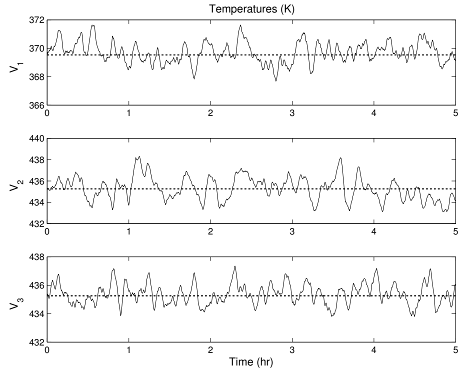

Fig. 4. Case 1: Q_2 "small" fault is isolated and control system is reconfigured to stabilize the closed-loop system - Temperatures.

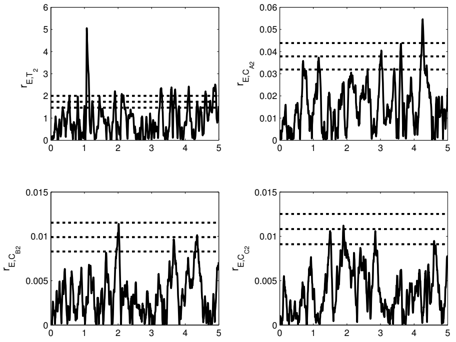

Fig. 5. Case 2: Q_2 "large" fault is isolated using shorter waiting time based on quick residual change of T_2. r_{E,T_2} immediately exceeds $\sigma_{T_2,5}$ at 1.060 hr where the fault is isolated and estimated within the waiting time of 36 s. The fault is estimated as 100 KJ/hr (actual 99 KJ/hr) at 1.070 hr

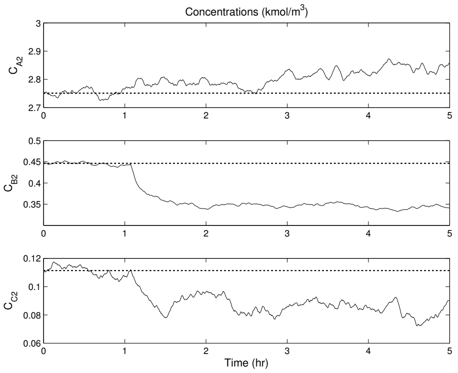

Fig. 6. Case 2: Q_2 "large" fault is isolated and control system is reconfigured to stabilize the closed-loop system - Concentrations.

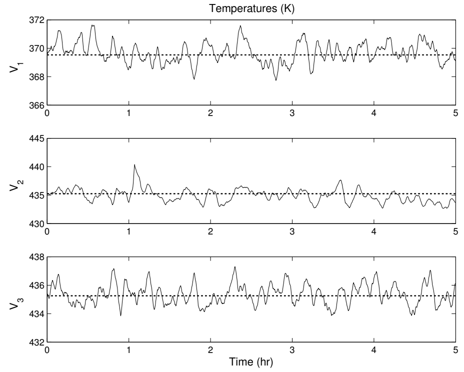

Fig. 7. Q_2 "large" fault is isolated and control system is reconfigured to stabilize the closed-loop system - Temperatures.

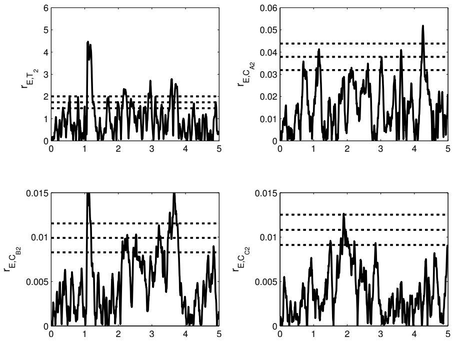

Fig. 8. Case 3: F_{20} fault demonstrates FDI system with multiple residual exceed thresholds. T_2 exceeds $\sigma_{T_2,3}$ at 1.070 hr and $\sigma_{T_2,5}$ at 1.075 hr and $r_{C_{B2}}$ exceeds $\sigma_{C_{B2},3}$ at 1.070 hr. The fault is isolated when $r_{C_{B2}}$ exceeds $\sigma_{C_{B2},5}$ at 1.075 hr and the fault is estimated to be 3.2 m^3/hr (actual 2.9 m^3/hr).

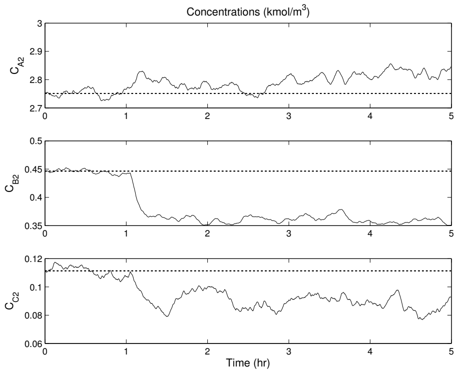

Fig. 9. Case 3: F_{20} fault is isolated and control system is reconfigured to stabilize the closed-loop system - Concentrations.

need for variable windows and minimum waiting times for proper isolation. Since both actuator faults considered affect the temperature in the second tank, the T_2 residual is used as the basis for determining the length of fault isolation time window. In case 3 an F_{20} fault occurs with a magnitude of 59% of $u_2^{\max}$. The T_2 residual exceeds $\sigma_{T_2,3}$ at 1.070 hr and $\sigma_{T_2,5}$ at 1.075 hr while the residual for concentration of component B in the second tank exceeds $\sigma_{C_{B2},3}$ at 1.070 hr. The fault is isolated since $r_{C_{B2}}$ exceeds $\sigma_{C_{B2},5}$ at 1.080 hr and the fault is estimated as 3.18 m^3/hr (actual 2.95 m^3/hr). The profiles of the states as the fault occurs and the FTC system reconfigures the control system is better seen in Fig. 8. Figures 9 and 10 show that the FTC system is able to stabilize the closed-loop system at a new steady-state after reconfiguration at 1.080 hr.

REFERENCES

[1] E. B. Ydstie, "New vistas for process control: Integrating physics and communication networks," *AIChE Journal*, vol. 48, pp. 422–426, 2002.

[2] P. D. Christofides, J. F. Davis, N. H. El-Farra, D. Clark, K. R. D. Harris, and J. N. Gipson, "Smart plant operations: Vision, progress and challenges," *AIChE Journal*, vol. 53, pp. 2734–2741, 2007.

[3] P. Mhaskar, A. Gani, N. H. El-Farra, P. D. Christofides, and J. F. Davis, "Integrated fault-detection and fault-tolerant control of process systems," *AIChE Journal*, vol. 52, pp. 2129–2148, 2006.

[4] N. H. El-Farra and S. Ghantasala, "Actuator fault isolation and reconfiguration in transport-reaction processes," *AIChE Journal*, vol. 53, pp. 1518–1537, 2007.

[5] K. Fukunaga, *Introduction to statistical pattern recognition*. New York: Academic Press, 1990.

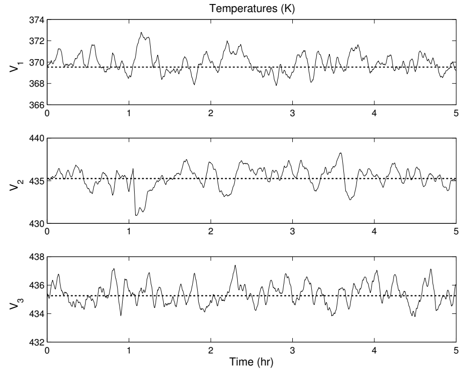

Fig. 10. Case 3: F_{20} fault is isolated and control system is reconfigured to stabilize the closed-loop system - Temperatures.

[6] P. Mhaskar, C. McFall, A. Gani, P. D. Christofides, and J. F. Davis, "Isolation and handling of actuator faults in nonlinear systems," *Automatica*, vol. 44, pp. 53–62, 2008.

[7] E. Camponogara, D. Jia, B. H. Krogh, and S. Talukdar, "Distributed model predictive control," *IEEE Control Systems Magazine*, vol. 22, pp. 44–52, 2002.

[8] J. B. Rawlings and B. T. Stewart, "Coordinating multiple optimization-based controllers: New opportunities and chanllenges," in *Procedings of the 8th IFAC Symposium on Dynamics and Control of Process*, vol. 1, Cancun, Mexico, 2007, pp. 19–28.

[9] R. Scattolini, "Architectures for distributed and hierarchical model predictive control - A review," *Journal of Process Control*, vol. 19, pp. 723–731, 2009.

[10] J. M. Maestre, D. Muñoz de la Peña, and E. F. Camacho, "A distributed MPC scheme with low communication requirements," in *Proceedings of the American Control Conference*, Saint Louis, MO, USA, 2009, pp. 2797–2802.

[11] J. Liu, D. Muñoz de la Peña, and P. D. Christofides, "Distributed model predictive control of nonlinear process systems," *AIChE Journal*, vol. 55, pp. 1171–1184, 2009.

[12] J. Liu, X. Chen, D. Muñoz de la Peña, and P. D. Christofides, "Sequential and iterative architectures for distributed model predictive control of nonlinear process systems," *AIChE Journal*, vol. 56, pp. 2137–2149, 2010.

[13] D. Chilin, J. Liu, D. Muñoz de la Peña, P. D. Christofides, and J. F. Davis, "Detection, isolation and handling of actuator faults in distributed model predictive control systems," *Journal of Process Control*, vol. 20, pp. 1059–1075, 2010.

[14] Y. Lin, E. D. Sontag, and Y. Wang, "A smooth converse Lyapunov theorem for robust stability," *SIAM Journal on Control and Optimization*, vol. 34, pp. 124–160, 1996.

[15] P. D. Christofides and N. H. El-Farra, *Control of nonlinear and hybrid process systems: Designs for uncertainty, constraints and time-delays*. Berlin, Germany: Springer-Verlag, 2005.

[16] B. Ohran, D. Muñoz de la Peña, P. D. Christofides, and J. F. Davis, "Enhancing data-based fault isolation through nonlinear control," *AIChE Journal*, vol. 53, pp. 2734–2741, 2008.

[17] J. M. Lucas and M. S. Saccucci, "Exponentially weighted moving average control schemes: Properties and enhancements," *Technometrics*, vol. 32, pp. 1–12, 1990.