2008 American Control Conference
Westin Seattle Hotel, Seattle, Washington, USA
June 11-13, 2008

Robust Diagnosis and Fault-Tolerant Control of Uncertain Distributed Processes with Limited Measurements

Sathyendra Ghantasala and Nael H. El-Farra†
Department of Chemical Engineering & Materials Science
University of California, Davis, CA 95616 USA

Abstract— **This work develops a robust fault detection and isolation (FDI) and fault-tolerant control (FTC) structure for distributed processes modeled by nonlinear parabolic PDEs with control constraints, time-varying uncertain variables and a finite number of output measurements with limited accuracy. To facilitate the controller synthesis and fault diagnosis tasks, a finite-dimensional system that approximates the dominant dynamic modes of the PDE is initially derived and transformed to a form where each dominant mode is excited directly by only one actuator. A robustly stabilizing bounded output feedback controller is then designed for each dominant mode. The controller synthesis procedure facilitates the derivation of (1) an explicit characterization of the fault-free behavior of each mode in terms of a time-varying bound on the dissipation rate of the corresponding Lyapunov function which accounts for the uncertainty and measurement errors, and (2) an explicit characterization of the robust stability region where constraint satisfaction and robustness with respect to uncertainty and measurement errors are guaranteed. Using the fault-free Lyapunov dissipation bounds as thresholds for FDI, the detection and isolation of faults in a given actuator is accomplished by monitoring the evolution of the dominant modes within the corresponding stability region and declaring a fault when the threshold is exceeded. Robustness of the FDI scheme to measurement errors is ensured by confining the FDI region to an appropriate subset of the stability region, and enlarging the FDI thresholds appropriately. It is shown that these safeguards can be tuned by appropriate selection of the sensor configuration. Finally, the implementation of the FTC architecture on the infinite-dimensional system is discussed and the proposed methodology is demonstrated using a diffusion-reaction process example.**

I. INTRODUCTION

The problems of fault detection and isolation (FDI) and fault-tolerant control (FTC) of dynamic systems have been the focus of considerable research interest over the past few decades in both the academic and industrial circles (e.g., see [1], [2], [3], [4], [5], [6], [7], [8] and the references therein). Despite the extensive literature on these topics, most of the available results have been developed for spatially homogeneous processes modeled by systems of ordinary differential equations. Many important engineering systems, however, such as transport-reaction processes and fluid flows, are characterized by spatial variations and are modeled by Partial Differential Equations (PDEs). While the study of these systems has been an area of significant and growing interest within process control research over the past decade (e.g., see [9], [10], [11] and the references therein), the development of systematic methods for the diagnosis and handling of faults in distributed control systems has received limited attention. Examples of earlier works in this direction include the development of fault detection schemes using approximate linear models (e.g., [12], [13]) and the use of hybrid system formulations to develop stability-based and performance-based controller reconfiguration strategies to compensate for faults (e.g., [14]). More recently, we developed in [15], [16] a unified framework for the integration of model-based FDI and control system reconfiguration for distributed processes modeled by nonlinear parabolic PDEs with control constraints and actuator faults. A key idea in these works is to tie the design of the FDI filters and the actuator reconfiguration logic via singular perturbations to the two time-scale separation between the slow and fast eigenvalues of the differential operator of the infinite-dimensional system, which leads naturally to the derivation of explicit FDI thresholds and actuator reconfiguration rules that minimize false and missed alarms due to approximation errors when the low-order model-based architecture is implemented on the distributed parameter system. These results were subsequently extended in [17], [18] to address the problem of model uncertainty. The central idea was to shape the fault-free closed-loop behavior, via robust bounded state feedback control, in a specific way that facilitates the derivation of FDI rules that are less sensitive to the uncertainty.

The implementation of the schemes mentioned above requires the availability of accurate measurements of the state variables at all points in the spatial domain. In practice, however, measurements of the state variables in a spatially-distributed system are typically available only at a finite number of spatial locations. Furthermore, accurate measurements are often unavailable due to the presence of measurement noise, the occurrence of sensor malfunctions, or the inherent limitations on the capabilities of the sensing device as in discrete sensors that provide only a limited (i.e., qualitative) information about the state of the system. These practical limitations can seriously erode the diagnostic and fault-tolerance capabilities of the fault-tolerant control architecture, if not explicitly accounted for in its design. Within the feedback control layer, for example, measurement errors can degrade the stability and performance properties of the nominal controllers and may render the closed-loop system unstable unless the

† To whom correspondence should be addressed: E-mail: nhelfarra@ucdavis.edu. Financial support by The Petroleum Research Fund administered by The American Chemical Society, ACS-PRF 47072-G9, is gratefully acknowledged.

controller is designed with a sufficient robustness margin. At the fault diagnosis level, the presence of measurement errors limits our ability to accurately monitor the actual evolution of the process to determine if and when a fault can be declared. Unless the FDI rules are re-designed to discriminate between those errors and faults, the FDI scheme may lead to false alarms that trigger unnecessary control system reconfiguration. The lack of full or accurate state measurements also limits the size of the stability regions as well as the supervisor's knowledge of where the system trajectory is relative to those regions. This in turn complicates the actuator reconfiguration task.

Motivated by these considerations, we develop in this work a robust fault diagnosis and fault-tolerant control structure for distributed processes modeled by nonlinear parabolic PDEs with control constraints, time-varying uncertain variables and a finite number of output measurements with limited accuracy. The structure consists of a family of robust output feedback controllers with well-characterized stability and robustness properties, a set of performance-based FDI rules that are less sensitive to the uncertainty and measurement errors, and a set of robust switching laws that orchestrate stabilizing transitions from the faulty actuators to the healthy fall-backs following FDI. The various components are designed on the basis of an approximate, finite-dimensional system that captures the PDE's dominant dynamic modes. The rest of the paper is organized as follows. Following some preliminaries in Section II, the approximate, finite-dimensional system is obtained in Section III and used in Section IV to construct the FDI-FTC structure and analyze its robustness to measurement errors. The implementation of the proposed architecture on the infinite-dimensional system is also discussed. Finally, the results are applied in Section V to achieve fault-tolerant stabilization of an unstable steady-state of a representative diffusion-reaction process. Due to space limitations, the proofs for the main results are omitted here and can be found in the full version of this work [19].

II. PRELIMINARIES

We consider spatially distributed processes modeled by nonlinear parabolic PDEs of the form:

$$\frac{\partial \bar{x}}{\partial t} = \alpha\frac{\partial^2 \bar{x}}{\partial z^2} + f(\bar{x}) + \omega\sum_{i=1}^{m} b_i^{k(t)}(z)[u_i^{k(t)} + f_{a_i}^{k(t)}] + \sum_{j=1}^{q} w_j(\bar{x})d_j(z)\theta_j(t),\ k(t) \in \mathcal{I} := \{1, 2, \cdots, N\} \tag{1}$$

$$|u_i^k(t)| \le u_{i,\max}^k,\ i = 1, \cdots, m,\ |\theta(t)| \le \theta_b \tag{2}$$

$$y_j(t) = \int_0^{\pi} q_j(z)\bar{x}(z,t)dz + s_j(t),\ j = 1, \cdots, n,\ |s(t)| \le \mu \tag{3}$$

subject to the boundary and initial conditions:

$$\bar{x}(0,t) = \bar{x}(\pi,t) = 0, i = 1, 2;\ \bar{x}(z,0) = \bar{x}_0(z) \tag{4}$$

where $\bar{x}(z,t) \in \mathbb{R}$ denotes the state variable, $z \in [0,\pi] \subset \mathbb{R}$ is the spatial coordinate, $t \in [0,\infty)$ is the time, $f(\cdot)$ and $w_j(\cdot)$ are smooth nonlinear functions, $\theta_j(t) \in \mathbb{R}$ denotes an uncertain variable, which may include uncertain process parameters or exogenous disturbances, $d_j(\cdot)$ is a known function that specifies the positions of action of the uncertain variable, u_i^k denotes the i-th manipulated input (control actuator) associated with the k-th control configuration, $b_i^k(\cdot)$ is a function that describes how the control action is distributed in $[0,\pi]$, $f_{a_i}^k \in \mathbb{R}$ denotes a fault in the i-th actuator of the k-th control configuration, $k(t)$ is a discrete variable that takes values in a finite set $\mathcal{I}$ and denotes which control configuration is active at any given time, N is the number of control configurations available, where each configuration has a distinct spatial placement of actuators (only one configuration is active at any given time), $|\cdot|$ is the standard Euclidean norm, $u_{i,\max}^k$ is a positive real number that captures the size of actuator constraints, θ_b is a known bound on the size of the uncertainty, $y_j(t) \in \mathbb{R}$ is a measured output, $q_j(\cdot)$ is a function that describes how the measurement output is distributed in $[0,\pi]$, $s_j(t)$ is an error in the j-th measurement reflecting the limited accuracy of the j-th sensor, $s = [s_1\ s_2\ \cdots\ s_n]'$, μ is a known bound on the size of the measurement error, the parameter $\alpha > 0$ is a constant, and $\bar{x}_0(z)$ is a smooth function of z. Throughout the paper, the notations $\|\cdot\|$ and $\|\cdot\|_2$ will be used to denote the L_2 norms associated with a finite-dimensional and infinite-dimensional Hilbert spaces, respectively, with inner product $\langle\omega_1, \omega_2\rangle = \int_0^{\pi}\omega_1(z)\omega_2(z)dz$.

The PDE of Eqs.1-4 can be formulated as an infinite-dimensional system of the form:

$$\begin{aligned} \dot{x} &= \mathcal{A}x + \mathcal{B}^k(u^k + f_a^k) + f(x) + \mathcal{W}(x)\theta,\ x(0) = x_0 \\ y &= \mathcal{Q}x + s \end{aligned} \tag{5}$$

where $x(t) = \bar{x}(z,t)$, $t > 0$, $0 < z < \pi$, is the state function defined on an appropriate Hilbert space $\mathcal{H} = L_2(0,\pi)$, $\mathcal{A}$ is the differential operator, $\mathcal{B}^k$ and $\mathcal{Q}$ are the input and output operators defined, respectively, as $\mathcal{B}^k(u^k + f_a^k) = \omega\sum_{i=1}^{m} b_i^{k(t)}(z)[u_i^{k(t)} + f_{a_i}^{k(t)}]$ and $\mathcal{Q}x(t) = [\langle q_1, x(t)\rangle\ \ \langle q_2, x(t)\rangle\ \ \cdots\ \ \langle q_n, x(t)\rangle]'$, where $u^k = [u_1^k\ u_2^k\ \cdots\ u_m^k]'$ and $f_a^k = [f_{a,1}^k\ f_{a,2}^k\ \cdots\ f_{a,m}^k]'$, $f(x(t)) = f(\bar{x}(z,t))$, $\mathcal{W}$ is the uncertainty operator, $\theta = [\theta_1 \cdots \theta_q]'$, and $x_0 = \bar{x}_0(z)$. We assume that $f(\cdot)$ is locally Lipschitz and satisfies $f(0) = 0$. For $\mathcal{A}$, the eigenvalue problem is defined as: $\mathcal{A}\psi_j = \lambda_j\psi_j,\ j = 1, \ldots, \infty$, where λ_j denotes an eigenvalue and ψ_j denotes an eigenfunction. By solving this eigenvalue problem, it can be shown that all the eigenvalues of $\mathcal{A}$ are real and ordered. Also, only a finite number of unstable eigenvalues exists, and the distance between two consecutive eigenvalues (i.e., λ_j and λ_{j+1}) increases as j increases. Furthermore, the spectrum of $\mathcal{A}$ can be partitioned as $\sigma(\mathcal{A}) = \sigma_1(\mathcal{A}) \bigcup \sigma_2(\mathcal{A})$, where $\sigma_1(\mathcal{A}) = \{\lambda_1, \cdots, \lambda_m\}$ contains the first m (with m finite) "slow" eigenvalues and $\sigma_2(\mathcal{A}) = \{\lambda_{m+1}, \lambda_{m+2}, \cdots\}$ contains the remaining "fast" stable eigenvalues where $|\lambda_m|/|\lambda_{m+1}| = O(\epsilon)$ and $\epsilon < 1$ is a small positive number characteristic of the large separation between the slow and fast eigenvalues of $\mathcal{A}$. This implies that the dominant dynamics of the PDE can be described by a finite-dimensional system, and motivates the use of modal decomposition in the next section to derive such a system.

III. Modal decomposition

Let $\mathcal{H}_s$, $\mathcal{H}_f$ be modal subspaces of $\mathcal{A}$, defined as $\mathcal{H}_s = \text{span}\{\psi_1, \ldots, \psi_m\}$ and $\mathcal{H}_f = \text{span}\{\psi_{m+1}, \psi_{m+2}, \ldots\}$. Defining the orthogonal projection operators, $\mathcal{P}_s$ and $\mathcal{P}_f$, such that $x_s = \mathcal{P}_s x$, $x_f = \mathcal{P}_f x$, the state of the system of Eq.5 can be decomposed as $x = x_s \bigoplus x_f$. Applying $\mathcal{P}_s$ and $\mathcal{P}_f$ to the system of Eq.5 and using the decomposition of x, the system of Eq.5 can be decomposed as:

$$\dot{x}_s = F_s(x_s, x_f) + \mathcal{B}_s^k(u^k + f_a^k) + \mathcal{W}_s(x_s, x_f)\theta \quad (6)$$

$$\dot{x}_f = F_f(x_s, x_f) + \mathcal{B}_f^k(u^k + f_a^k) + \mathcal{W}_f(x_s, x_f)\theta \quad (7)$$

$$y = \mathcal{Q}x_s + \mathcal{Q}x_f + s \quad (8)$$

where $x_s(0) = \mathcal{P}_s x_0$, $x_f(0) = \mathcal{P}_f x_0$, $F_s(x_s, x_f) = \mathcal{A}_s x_s + f_s(x_s, x_f)$, $\mathcal{A}_s = \mathcal{P}_s\mathcal{A}$ is an $m \times m$ diagonal matrix of the form $\mathcal{A}_s = \text{diag}\{\lambda_j\}$, $\mathcal{B}_s = \mathcal{P}_s\mathcal{B}$, $f_s = \mathcal{P}_s f$, $\mathcal{W}_s = \mathcal{P}_s\mathcal{W}$, $F_f(x_s, x_f) = \mathcal{A}_f x_f + f_f(x_s, x_f)$, $\mathcal{A}_f = \mathcal{P}_f\mathcal{A}$ is an unbounded differential operator which is exponentially stable, $\mathcal{B}_f = \mathcal{P}_f\mathcal{B}$, $f_f = \mathcal{P}_f f$ and $\mathcal{W}_f = \mathcal{P}_f\mathcal{W}$. We will refer to the x_s- and x_f-subsystems as the slow and fast subsystems, respectively. Neglecting the fast and stable x_f-subsystem of Eq.7, the following approximate, m-dimensional slow system is obtained:

$$\begin{aligned} \dot{\bar{x}}_s &= F_s(\bar{x}_s, 0) + \mathcal{B}_s^k(u^k + f_a^k) + \mathcal{W}_s(\bar{x}_s, 0)\theta \\ \bar{y} &= \mathcal{Q}\bar{x}_s + s \end{aligned} \quad (9)$$

where the bar symbols denote that these variables are associated with a finite-dimensional system. To facilitate the controller synthesis and simplify closed-loop analysis, we will consider in the remainder of the paper that the inverse (or pseudo-inverse in the case of a non-square system) of the operator $\mathcal{Q}$ exists. This requirement, which can be met by appropriate choice of the locations of the sensors, allows obtaining estimates of the state of the system of Eq.9 from the measurements, $\widetilde{x}_s = \mathcal{Q}^{-1}\bar{y}$. Beyond making the robustness analysis more transparent, the choice to use static output feedback also allows practically preserving the stability region of any stabilizing bounded controller (designed based on the approximate system of Eq.9) when implemented on the infinite-dimensional system (see [14] for further discussion on this issue). It should be noted though that dynamic output feedback can also be used provided that a suitable observer can be found (e.g., [20]).

IV. FDI and FTC under uncertainty, constraints and measurement errors

This section presents the design methodology for the robust output feedback FDI-FTC structure on the basis of the system of Eq.9 and analyzes its robustness properties when implemented in the presence of measurement errors.

A. Bounded robust feedback control

In this section, we will first design the controllers assuming the availability of accurate output measurements and then analyze the effects of measurement errors to derive conditions for closed-loop stability.

1) Controller synthesis: To synthesize the controllers and facilitate FDI at the same time (see Section IV-B), the approximate system of Eq.9 is first transformed into the following form where the evolution of each dominant mode is directly influenced by only one actuator:

$$\dot{\bar{v}}_{s_i} = \bar{f}_{s_i}(\bar{v}_s) + \mathcal{D}_{s_i}^k[u_i^k + f_{a_i}^k] + \bar{\mathcal{W}}_{s_i}(\bar{v}_s)\theta, i = 1, \cdots, m \quad (10)$$

where $\bar{v}_{s_i}(t) := \mathcal{P}_{s_i}\bar{v}_s(t) \in \mathcal{H}_{s_i} = \text{span}\{\psi_i\}$, is the state of a one-dimensional system describing the evolution of the i-th slow mode in the transformed coordinates, $\mathcal{P}_{s_i}$ is the orthogonal projection operator that projects $\bar{v}_s(t) \in \mathcal{H}_s$ onto $\bar{v}_{s_i} \in \mathcal{H}_{s_i}$, $\bar{v}_s = \mathcal{T}_s^k(\xi_a^k)\bar{x}_s$, where $\mathcal{T}_s^k = \mathcal{B}_s^{k^{-1}}$ is the inverse (or pseudo-inverse in the case of a non-square system) of the input operator whose existence can be guaranteed by proper spatial placement of the control actuators, ξ_a^k is the vector of actuator locations in the k-th control configuration, $\mathcal{D}_{s_i}^k = \mathcal{P}_{s_i}\mathcal{T}_s^k\mathcal{B}_s^k$, $\bar{f}_{s_i} = \mathcal{P}_{s_i}\bar{f}_s$, $\bar{f}_s(\bar{v}_s) = \mathcal{T}_s^k F_s(\mathcal{T}_s^{k^{-1}}\bar{v}_s, 0)$, and $\bar{\mathcal{W}}_s(\bar{v}_s) = \mathcal{T}_s^k\mathcal{W}_s(\mathcal{T}_s^{k^{-1}}\bar{v}_s, 0)$. In the remainder of the section, we shall deal exclusively with the transformed system of Eq.10 with the understanding that the results also hold for the original system of Eq.9 due to the invertibility and boundedness of the transformation operator. We now proceed to design, for each dominant mode, a bounded robustly stabilizing controller on the basis of Eq.10. While several designs can be used to meet the desired control objectives, the following bounded robust control law (first introduced in [21] and inspired by the results in [22]) will be used as an example to illustrate the main ideas:

$$\begin{aligned} u_i^k &= p_i(\bar{v}_s, u_{i_{\max}}^k, \theta_b, \xi_{a_i}^k, \varrho_i) \\ &= -\psi_i^k(\bar{v}_s, u_{i_{\max}}^k, \theta_b, \xi_{a_i}^k, \varrho_i) L_{\mathcal{D}_{s_i}^k}\bar{V}_i, k \in \mathcal{I} \end{aligned} \quad (11)$$

where

$$\psi_i^k = \frac{\alpha_i(\bar{v}_s) + \sqrt{\alpha_i^2(\bar{v}_s) + \left(u_{i_{\max}}^k \beta_i^k(\bar{v}_{s_i}, \xi_{a_i}^k)\right)^4}}{(\beta_i^k(\bar{v}_{s_i}, \xi_{a_i}^k))^2 \left[1 + \sqrt{1 + (u_{i_{\max}}^k \beta_i^k(\bar{v}_{s_i}, \xi_{a_i}^k))^2}\right]} \quad (12)$$

$\alpha_i(\cdot) = L_{\bar{f}_{s_i}}\bar{V}_i + \left(\rho_i\|\bar{v}_{s_i}\| + \chi_i\theta_b|L_{\bar{\mathcal{W}}_{s_i}}\bar{V}_i|\right)(\|\bar{v}_{s_i}\|/(\|\bar{v}_{s_i}\| + \bar{\phi}_i^k))$, $\beta_i^k(\cdot) = |L_{\mathcal{D}_{s_i}^k}\bar{V}_i|$, and $\bar{V}_i : \mathcal{H}_{s_i} \to \mathbb{R}_{\geq 0}$ is a robust control Lyapunov function [23] for the system of Eq.10 which, for simplicity, we take to be of the form $\bar{V}_i = \|\bar{v}_{s_i}\|^2$. The terms $L_{\bar{f}_{s_i}}\bar{V}_i$, $L_{\mathcal{D}_{s_i}^k}\bar{V}_i$ and $L_{\bar{\mathcal{W}}_{s_i}}\bar{V}_i$ are Lie derivatives of $\bar{V}_i$, and $\varrho_i = [\rho_i\ \chi_i\ \bar{\phi}_i]'$ is a vector of adjustable parameters with $\rho_i > 0$, $\chi_i > 1$, $\bar{\phi}_i > 0$. Let $\bar{\Pi}_i^k$ be the set defined by:

$$\bar{\Pi}_i^k := \{\bar{v}_s \in \mathcal{H}_s : \alpha_i^k(\bar{v}_s, \varrho_i, \theta_b) \leq u_{i_{\max}}^k \beta_i^k(\bar{v}_{s_i}, \xi_{a_i}^k)\} \quad (13)$$

and let $\bar{\Pi}^k := \bigcap_{i \in \mathcal{I}} \bar{\Pi}_i^k$ be the intersection of all $\bar{\Pi}_i^k$, then it can be shown, using a standard Lyapunov argument, that if $\bar{v}_s(t) \in \bar{\Pi}_i^k$, for some $t \geq 0$, there exists positive real numbers, γ_i, $\tilde{\phi}_i$, and a class $\mathcal{K}$ function $\sigma_i(\cdot)$[1] such that if $\phi_i := \bar{\phi}_i(\chi_i - 1)^{-1} \leq \tilde{\phi}_i$, the time-derivative of $\bar{V}_i$ along the trajectories of the closed-loop system of Eqs.10-12, with $f_{a_i}^k \equiv 0$ for a given i and $s \equiv 0$, satisfies:

$$\dot{\bar{V}}_i(t) \leq -\gamma_i\bar{V}_i(t) + \sigma_i(\phi_i) \quad (14)$$

[1]A continuous real-valued function is said to be of class $\mathcal{K}$ if it is monotonically non-decreasing and is zero at zero.

Furthermore, if $f_{a_i}^k \equiv 0$ for all i and $\bar{v}_s(0) \in \bar{\Omega}_s^k(\theta_b, u_{\max}^k, \xi^k)$, where:

$$\bar{\Omega}_s^k(\theta_b, u_{\max}^k, \xi_{a_i}^k) := \{\bar{v}_s \in \bar{\Pi}^k : \bar{V}(\bar{v}_s) \le \bar{\delta}_s\} \tag{15}$$

for some $\bar{\delta}_s > 0$, where $\bar{V} = \sum_{i=1}^m \bar{V}_i$ is a composite Lyapunov function for the entire system, then for every real number $\bar{\delta}_{d_i} > 0$, there exists ϕ_i^* such that if $\phi_i \in (0, \phi_i^*]$, $\limsup_{t\to\infty} \bar{V}_i(\bar{v}_{s_i}(t)) \le \bar{\delta}_{d_i}$, for $i = 1, \cdots, m$, and the origin of the closed-loop system is practically stable.

2) Robustness to measurement errors: Referring to the systems of Eqs.9-10 with $s \neq 0$, let $\widetilde{v}_s = \mathcal{T}_s^k(\xi_a^k)\widetilde{x}_s = \mathcal{T}_s^k(\xi_a^k)\mathcal{Q}^{-1}(\xi_s)\bar{y}$ be the estimate used to implement the controllers of Eqs.11-12. From the bound on the measurement error given in Eq.3, $|s(t)| \le \mu$, and the fact that $\widetilde{v}_s = \bar{v}_s + \mathcal{T}_s^k(\xi_a^k)\mathcal{Q}^{-1}(\xi_s)s$, the following bound on the estimation error can be obtained:

$$\|\widetilde{v}_s - \bar{v}_s\| \le E(\xi_a^k, \xi_s)\mu := \mu^*(\xi_a^k, \xi_s, \mu) \tag{16}$$

where $E(\xi_a^k, \xi_s) = \|\mathcal{T}_s^k(\xi_a^k)\|\|\mathcal{Q}^{-1}(\xi_s)\|$. Furthermore, from the continuity of the control law, $p_i(\cdot)$, it follows that given any positive real number μ^* there exists a class $\mathcal{K}$ function $M_i(\cdot)$ such that if $\|\widetilde{v}_s - \bar{v}_s\| \le \mu^*$, $|p_i(\widetilde{v}_s) - p_i(\bar{v}_s)| \le M_i(\mu^*)$. Now, consider the subset defined by $\widetilde{\Pi}_i^k := \{\bar{v}_s \in \bar{\Pi}_i^k : |p_i^k(\bar{v}_s)| \le u_{i,\max}^k - M_i(\mu^*)\}$ and let $\widetilde{\Pi}^k := \bigcap_{i=1,\cdots,m} \widetilde{\Pi}_i^k$. Also, let $\widetilde{\Omega}_s^k(\theta_b, u_{\max}^k, \xi_a^k, \mu^*) := \{\bar{v}_s \in \widetilde{\Pi}^k : \bar{V}(\bar{v}_s) \le \widetilde{\delta}_s\}$, for some $\widetilde{\delta}_s > 0$. The following proposition characterizes the stability properties of the closed-loop system under bounded measurement errors and in the absence of faults.

Proposition 1: *Consider the closed-loop system of Eqs.10-12, for a fixed $k \in \mathcal{I}$, with $f_{a_i}^k \equiv 0$ for a given i. Then, if $\bar{v}_s(t) \in \widetilde{\Pi}_i^k$, there exist positive real numbers, γ_i, $\tilde{\phi}_i$, and class $\mathcal{K}$ functions, $\sigma_i(\cdot)$ and $\Xi_i(\cdot)$, such that if $\phi_i \le \tilde{\phi}_i$, the time-derivative of $\bar{V}_i$ along the trajectories of Eq.10 satisfies:*

$$\dot{\bar{V}}_i(t) \le -\gamma_i \bar{V}_i(t) + \sigma_i(\phi_i) + \Xi_i(\mu^*) \tag{17}$$

and $|p_i(\widetilde{v}_s(t))| \le u_{i,\max}^k$. Furthermore, if $f_{a_i}^k \equiv 0$ for all i, then for every pair of positive real numbers $\{\bar{\delta}_{d_i}, a\}$ such that $a \in (0,1)$ and $\widetilde{\delta}_{d_i} := a^{-1}\gamma_i^{-1}(\bar{\delta}_{d_i} + \Xi_i(\mu^*)) < \widetilde{\delta}_{s_i}$, where $\sum_{i=1}^m \widetilde{\delta}_{s_i} = \widetilde{\delta}_s$, there exists ϕ_i^* such that if $\phi_i \in (0, \phi_i^*]$ and $\bar{v}_s(0) \in \widetilde{\Omega}_s^k$, $\limsup_{t\to\infty} \bar{V}_i(t) \le \widetilde{\delta}_{d_i} < \widetilde{\delta}_{s_i}$, for $i = 1, \cdots, m$, and the origin of the closed-loop system is practically stable.

The set $\widetilde{\Omega}_s^k(u_{max}^k, \theta_b, \xi_a^k, \xi_s)$ represents an estimate of the robust stability region for the k-th fault-free actuator configuration, starting from where each output feedback controller (implemented with measurement errors) satisfies the constraints and drives the trajectory of its corresponding mode in finite-time into a small neighborhood of the origin (residual set) where it remains confined for all future times. The size of each residual set, $\widetilde{\delta}_{d_i}$, is determined by (1) the desired degree of uncertainty attenuation (which can be made arbitrarily small provided the controller is tuned properly) and (2) the size of the estimation error which is fixed in part by the measurement errors. For the problem to be well-posed, the errors in the measurements should not be larger than the measurements themselves. This is captured by the requirement that $\widetilde{\delta}_{d_i} := a^{-1}\gamma_i^{-1}(\bar{\delta}_{d_i} + \Xi_i(\mu^*)) < \widetilde{\delta}_{s_i}$ which ensures that the union of all residual sets is contained within the stability region and that the closed-loop trajectories remain bounded for all times.

Remark 1: In addition to its dependence on the size of the constraints, the size of uncertainty and the locations of the control actuators, the set $\widetilde{\Omega}_s^k$ is also parameterized by the locations of the measurement sensors. Confining the states within this set ensures that estimation errors do not cause the output feedback controllers to compute control actions that violate the specified constraints. Similarly, the size of each residual set is also a function of the sensor locations. Therefore, while the presence of measurement errors leads to shrinkage in the stability region and enlargement of the residual sets (relative to the case of error-free measurements), it is possible to get a handle on the extent of these changes by proper selection of the sensor configuration.

B. Rules for robust actuator fault detection and isolation

The fact that the bound of Eq.17 is valid for a given mode regardless of the fault or health status of the actuators associated with the other modes (as long as $\bar{v}_s$ is within $\widetilde{\Omega}_s^k$) implies that it can be used as a threshold for FDI. This threshold, however, cannot be used directly to derive the FDI rules since it requires monitoring the state which is known with only limited accuracy due to the presence of measurement errors. The following proposition describes how to obtain the needed threshold in terms of the estimate $\widetilde{v}_s$ instead, and how to use it for FDI.

Proposition 2: *Consider the closed-loop system of Eqs.10-12, for a fixed $k \in \mathcal{I}$, with $f_{a_i}^k \equiv 0$ and $\phi_i \in (0, \phi_i^*]$ for a given i. Let $\widetilde{\Omega}_c^k := \{\widetilde{v}_s \in \widetilde{\Pi}^k : \bar{V}(\widetilde{v}_s) \le \widetilde{\delta}_c\}$, where $\sqrt{\widetilde{\delta}_c} + \mu^*(\xi_s, \xi_a, \mu) < \sqrt{\widetilde{\delta}_s}$. Then, if $\widetilde{v}_s(t) \in \widetilde{\Omega}_c^k$, for some $t \ge 0$, there exists a class $\mathcal{K}$ function $\Delta_i(\mu^*) > \Xi_i(\mu^*)$ such that, for some $a \in (0,1)$, the time-derivative of $\widetilde{V}_i := \|\widetilde{v}_{s_i}\|^2$ satisfies: (a) $\dot{\widetilde{V}}_i(t) \le -(1-a)\gamma_i \widetilde{V}_i(t)$ if $\widetilde{V}_i(t^-) \ge \widetilde{\delta}_{p_i}$, and (b) $\widetilde{V}_i(t) \le \widetilde{\delta}_{p_i}$ if $\widetilde{V}_i(t^-) \le \widetilde{\delta}_{p_i}$, where $\widetilde{\delta}_{p_i} := a^{-1}\gamma_i^{-1}(\bar{\delta}_{d_i} + \Delta_i(\mu^*))$ and $\bar{\delta}_{d_i}$ is defined in Proposition 1.*

The expected fault-free evolution of the state estimates characterized in Proposition 2 can be used to derive rules for actuator FDI under uncertainty and measurement errors. Two cases can be distinguished here. The first is when $\widetilde{v}_{s_i}$ lies outside its residual set, i.e., $\widetilde{\delta}_{p_i} < \widetilde{V}_i(t^-) \le \widetilde{\delta}_{s_i}$ for some $a \in (0,1)$. In this case, faults in the i-th actuator that cause an increase in $\widetilde{V}_i$ (destabilizing faults) and faults that slow down the decay rate of $\widetilde{V}_i$ beyond the minimum rate prescribed by the healthy robust controller, $\dot{\widetilde{V}}_i(t) > -(1-a)\gamma_i \widetilde{V}_i(t)$, (performance-degrading faults) will be detected and isolated. The second case is when, immediately prior to the fault, $\widetilde{v}_{s_i}$ lies within its residual set. In this case, a fault in the i-th actuator that causes $\widetilde{v}_{s_i}$ to begin to escape the residual set gets detected. In both cases, all the estimates have to be monitored to check if $\widetilde{v}_s(t)$ is within $\widetilde{\Omega}_c^k$ (which guarantees the validity of the fault-free bounds in Proposition 2). In this sense, $\widetilde{\Omega}_c^k$ can be interpreted as a region where robust FDI is feasible under constraints.

Remark 2: When comparing the above FDI rules with the ones obtained in the absence of measurement errors (i.e., with $\mu = 0$), we observe that Proposition 2 prescribes two modifications to safeguard against possible false alarms due to measurement errors. These include (1) limiting the FDI region to an appropriate subset of the stability region, $\widetilde{\Omega}_c^k$, and (2) enlarging the time-varying bounds on the dissipation of the Lyapunov functions beyond what is obtained in the error-free case. Given that $\bar{v}_s$ is known only with limited accuracy, the first modification is needed to provide a mechanism for inferring the location $\bar{v}_s$ by monitoring $\widetilde{v}_s$. Notice that $\widetilde{v}_s(t) \in \widetilde{\Omega}_c^k \Longrightarrow \bar{v}_s(t) \in \bar{\Omega}_s^k$ which is important to ensure the validity of the FDI rules (Eq.17). The second safeguard amounts to increasing the FDI alarm threshold (i.e., the size of the residual set) for each mode by a certain amount to ensure that any potential discrepancy between the actual and expected behavior is more than what can be accounted for by estimation errors, and thus is due solely to faults in a given actuator. Again, for the problem to be well-posed, the new (larger) residual sets must be contained within the FDI region, i.e., $\widetilde{\delta}_{p_i} < \widetilde{\delta}_{c_i}$ which imposes a limit on the size of the tolerable measurement errors. Finally, the dependence of $\widetilde{\delta}_c$ and $\widetilde{\delta}_{p_i}$ on the sensor locations offers a degree of freedom that can be used to limit the extent of the necessary modifications in the FDI and residual regions.

C. Robust stability-based actuator reconfiguration

Following FDI, the supervisor needs to determine which backup configuration to activate to maintain closed-loop stability. To this end, consider the system of Eq.10 where (1) for each control configuration a family of robust controllers have been designed and the corresponding monitoring regions have been characterized, and (2) given the bound on measurement errors, the achievable level of ultimate boundedness, $\widetilde{\delta}_d$, has been determined. The following theorem describes the integration of FDI and actuator reconfiguration to ensure fault-tolerance in the closed-loop system.

Theorem 1: *Consider the closed-loop system of Eqs.10-12 with $k(0) = j \in \mathcal{I}$, $\bar{v}_s(0) \in \widetilde{\Omega}_s^j$. Let $T_d := \min\{t : f_{a_i}^j(t) \neq 0\}$, for some i, then the switching rule:*

$$k(t)= \begin{cases} j, & 0 \leq t < T_d \\ \nu \neq j,\, t \geq T_d, \widetilde{v}_s(T_d) \in \widetilde{\Omega}_c^\nu, \xi_{a_r}^\nu = \xi_{a_r}^j, r \neq i \end{cases} \quad (18)$$

practically stabilizes the origin of the closed-loop system and $\limsup_{t\to\infty} \bar{V}_i(\bar{v}_{s_i}(t)) \leq \bar{\delta}_d$, for all $i = 1, \cdots, m$.

The switching law of Eq.18 ensures that: (1) the fall-back actuator configuration activated following FDI guarantees robust closed-loop stability and the desired level of ultimate boundedness (this follows from the requirement $\widetilde{v}_s(T_d) \in \widetilde{\Omega}_c^\nu$ which guarantees $\bar{v}_s(T_d) \in \widetilde{\Omega}_s^\nu$), and (2) only the faulty actuators of the operating configuration are switched out while the healthy ones are kept active.

Remark 3: It can be shown that the above FDI-FTC architecture continues to ensure stability and retain the fault-tolerance capabilities when implemented on the infinite dimensional system, provided that the separation between the slow and fast eigenvalues of the differential operator is sufficiently large and the FDI rules are slightly modified. Specifically, the closeness of solutions between the approximate and infinite-dimensional systems can be exploited to show that Eq.14 continues to hold up to an arbitrarily small offset provided that ϵ (which is inversely proportional to the separation between the slow and fast eigenvalues) is small enough. This leads to modified FDI thresholds that are $O(\epsilon)$ close to the bounds obtained for the approximate system, and ensure robustness against approximation errors. This argument can be justified using singular perturbation techniques (see [19] for the mathematical details).

V. Application to a diffusion-reaction process

Consider a diffusion-reaction process modeled by the following parabolic PDE:

$$\begin{aligned} \frac{\partial \bar{x}}{\partial t} &= \frac{\partial^2 \bar{x}}{\partial z^2} + (\beta_T + \theta_1(t)) \left[e^{-\gamma/(1+\bar{x})} - e^{-\gamma} \right] - \beta_U \bar{x} \\ &+ \beta_U \textstyle\sum_{i=1}^{3} b_i(z)[u_i(t) + f_{a_i}(t)] + \beta_U d(z)\theta_2(t) \end{aligned}$$

subject to $\bar{x}(0,t) = \bar{x}(\pi,t) = 0$, where $\bar{x}$ denotes the dimensionless temperature, $\beta_T = 50.0$, $\beta_U = 2.0$, $\gamma = 2.0$ are dimensionless process parameters, $\theta_1(t) = 0.1\beta_T \sin(t)$ is a time-varying parametric uncertainty in the heat of reaction, and $\theta_2(t) = 0.01\sin(t)$ is a time-varying point-disturbance at $z_d = 0.125\pi$. It was verified that the operating steady-state $\bar{x}(z,t) = 0$ (with $u_i = 0$, $\theta_1 = \theta_2 = 0$) is unstable (the linearization around the zero solution has three positive eigenvalues). The control objective is to stabilize the temperature profile at this unstable, spatially uniform steady-state by manipulating the temperature of the cooling medium, u_i, under actuator constraints, faults, model uncertainty and inaccurate sensor measurements. To this end, three primary point control actuators, ($\xi_A = \pi/2, u_{\max}^A = 3.0$), ($\xi_B = \pi/3, u_{\max}^B = 2.0$) and ($\xi_C = \pi/6, u_{\max}^C = 2.0$), and five point measurement sensors with limited accuracy ($\xi_{s_1} = 0.1\pi, s_1 = y_1(1 - e^{-0.1t})$), ($\xi_{s_2} = 0.3\pi, s_2 = 0.8y_2(1 - e^{-0.1t})$), ($\xi_{s_3} = 0.4\pi, s_3 = 0.4y_3$), ($\xi_{s_4} = 0.6\pi, s_4 = 0.5y_3$), ($\xi_{s_5} = 0.8\pi, s_5 = 0.3y_5$), are assumed to be available. Three backup actuators, ($\xi_D = 3\pi/4, u_{\max}^D = 4.0$), ($\xi_E = 2\pi/5, u_{\max}^E = 4.0$), ($\xi_F = 2\pi/3, u_{\max}^F = 3.0$), are also available for use in the event of faults in the primary configuration (A, B, C).

The first three (unstable) eigenvalues are considered dominant and Galerkins method is applied to derive a third-order ODE system describing the approximate evolution of the amplitudes of the first three eigenmodes. This system is subsequently transformed into the form of Eq.10 and used for the synthesis of the output feedback controllers and the FDI rules which are implemented on a 30-th order Galerkin discretization of the PDE. The synthesis details are omitted due to space limitations. Fig.1 shows that, when implemented using actuator configuration (A, B, C) for all times with no failures, the controllers robustly stabilize the closed-loop system near the desired steady-state and suppress the effects of uncertainty and measurement errors.

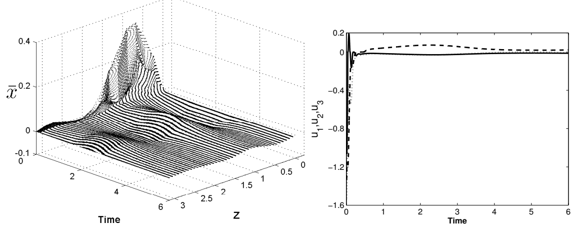

Fig. 1. Closed-loop state and manipulated input profiles with no faults.

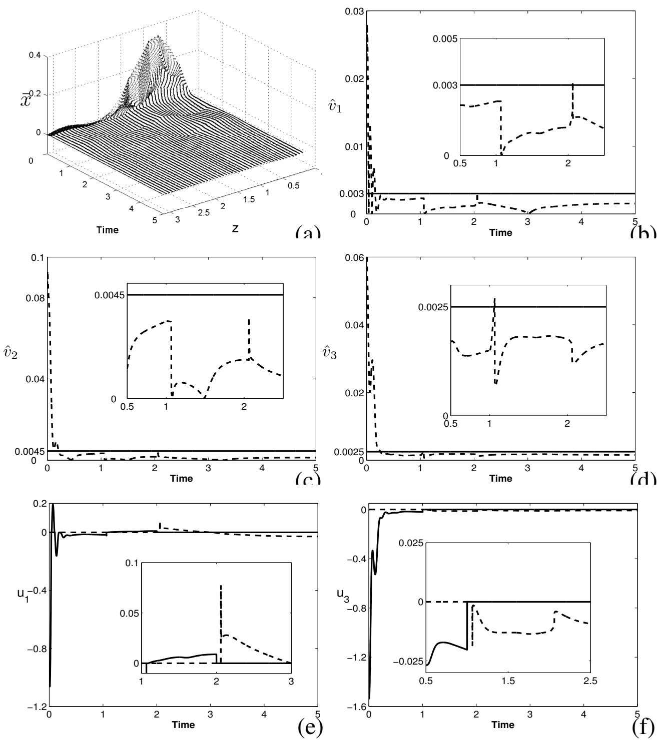

Fig. 2. Evolution of the closed-loop state (a), the estimates of the dominant modes' amplitudes (b)-(d), and manipulated input profiles (e)-(f) under consecutive failures and switching from C to D and A to E.

To demonstrate how the integrated FDI-FTC scheme works, we initialize the closed-loop system using configuration (A, B, C) which successfully drives all the dominant modes (and their estimates) into their prescribed residual sets very quickly (see Figs.2(a)-2(d)). Failure is then introduced into actuator C at $t = 1.0$. As shown in Fig.2(d), this failure is detected and isolated by the supervisor at $T_1 = 1.065$ since it causes only $\widehat{v}_3$ (dedicated to actuator C) to escape its terminal set ($|\widehat{v}_3(T_1)| > 0.0025$) at a time when the other estimates remain within their respective terminal sets, which is consistent with the fact that actuators A and B are healthy. Following FDI, the supervisor activates actuator D (see dashed line in Fig.2(f)) based on the switching logic of Eq.18 to preserve closed-loop stability. At $t = 2.0$, a failure in actuator A is introduced (see solid line in Fig.2(e)). This failure is detected and isolated when $\widehat{v}_1$ (dedicated to actuator A) begins to leave its terminal set at $T_2 = 2.06$ (Fig.2(b)), while $\widehat{v}_1$ and $\widehat{v}_3$ remain within their respective terminal sets. Following FDI, the supervisor activates actuator E (see dashed line in Fig.2(e)) in place of A which ensures closed-loop stability.

References

[1] D. M. Himmelblau, *Fault Detection and Diagnosis in Chemical and Petrochemical Processes*. New York: Elsevier Scientific Pub., 1978.

[2] P. M. Frank and X. Ding, "Survey of robust residual generation and evaluation methods in observer-based fault detection systems," *J. Proc. Contr.*, vol. 7, pp. 403–424, 1997.

[3] C. DePersis and A. Isidori, "A geometric approach to nonlinear fault detection and isolation," *IEEE Trans. Automat. Contr.*, vol. 46, pp. 853–865, 2001.

[4] E. Tatara and A. Cinar, "An intelligent system for multivariate statistical process monitoring and diagnosis," *ISA Transactions*, vol. 41, pp. 255–270, 2002.

[5] S. Simani, C. Fantuzzi, and R. Patton, *Model-based Fault Diagnosis in Dynamic Systems Using Identification Techniques*. London: Springer, 2003.

[6] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*. Berlin-Heidelberg: Springer, 2003.

[7] X. D. Zhang, T. Parisini, and M. M. Polycarpou, "Adaptive fault-tolerant control of nonlinear uncertain systems: An information-based diagnostic approach," *IEEE Trans. Automat. Contr.*, vol. 49, pp. 1259–1274, 2004.

[8] 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.

[9] P. D. Christofides, *Nonlinear and Robust Control of PDE Systems: Methods and Applications to Transport-Reaction Processes*. Boston: Birkhäuser, 2001.

[10] M. Ruszkowski, V. Garcis-Osorio, and B. E. Ydstie, "Passivity based control of transport reaction systems," *AIChE J.*, vol. 51, pp. 3147–3166, 2005.

[11] M. Demetriou and A. Armaou, "Robust detection and accommodation of incipient component faults in nonlinear distributed processes," in *Proceedings of American Control Conference*, New York, NY, 2007, pp. 2054–2059.

[12] H. Baruh, "Actuator failure detection in the control of distributed systems," *Journal of Guidance, Control, and Dynamics*, vol. 9, pp. 181–189, 1986.

[13] M. Demetriou, A. S. Ackleh, and S. Reich, "Detection and accommodation of second order distributed parameter systems with abrupt changes in the input term: Existence and approximation," *Kybernetika*, vol. 36, pp. 117–132, 2000.

[14] N. H. El-Farra and P. D. Christofides, "Coordinating feedback and switching for control of spatially-distributed processes," *Comp. & Chem. Eng.*, vol. 28, pp. 111–128, 2004.

[15] N. H. El-Farra, "Integrated fault detection and fault-tolerant control architectures for distributed processes," *Ind. & Eng. Chem. Res.*, vol. 45, pp. 8338–8351, 2006.

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

[17] S. Ghantasala and N. H. El-Farra, "Robust detection and handling of actuator faults in control of uncertain parabolic PDEs," *Journal of Dynamics of Continuous, Discrete and Impulsive Systems(Series A)*, vol. 14, pp. 203–208, 2007.

[18] ——, "Detection, isolation and management of actuator faults in parabolic PDEs under uncertainty and constraints," in *Proceedings of 46th IEEE Conference on Decision and Control*, New Orleans, LA, 2007, pp. 878–884.

[19] ——, "Robust diagnosis and fault-tolerant control of distributed processes over communication networks," *International Journal of Adaptive Control and Signal Processing,* submitted, 2008.

[20] A. A. Alonso, C. E. Frouzakis, and I. G. Kevrekidis, "Optimal sensor placement for state reconstruction of distributed process systems," *AIChE J.*, vol. 50, pp. 1438–1452, 2004.

[21] N. H. El-Farra and P. D. Christofides, "Coordinating feedback and switching for control of hybrid nonlinear processes," *AIChE J.*, vol. 49, pp. 2079–2098, 2003.

[22] Y. Lin and E. D. Sontag, "A universal formula for stabilization with bounded controls," *Sys. & Contr. Lett.*, vol. 16, pp. 393–397, 1991.

[23] R. Freeman and P. V. Kokotovic, *Robust Nonlinear Control Design: State-Space and Lyapunov Techniques*. Boston: Birkhauser, 1996.