Actuator Fault Isolation and Reconfiguration in Transport-Reaction Processes

Nael H. El-Farra and Sathyendra Ghantasala
Dept. of Chemical Engineering and Materials Science, University of California, One Shields Avenue, Davis, CA 95616

DOI 10.1002/aic.11177
Published online May 7, 2007 in Wiley InterScience (www.interscience.wiley.com).

A methodology is presented for the design of integrated, model-based fault diagnosis and reconfigurable control systems for transport-reaction processes modeled by nonlinear parabolic partial differential equations (PDEs) with control constraints and actuator faults. The methodology brings together nonlinear feedback control, fault detection and isolation (FDI), and performance-based supervisory switching between multiple actuator configurations. Using an approximate, finite-dimensional model that captures the PDE's dominant dynamic modes, a stabilizing nonlinear feedback controller is initially designed for each actuator configuration, and its stability region is explicitly characterized in terms of the control constraints and actuator locations. To facilitate the fault diagnosis task, the locations of the control actuators are chosen in a way that ensures that the evolution of each dominant mode, in appropriately chosen coordinates, is excited by only one actuator. Then, a set of dedicated FDI filters, each replicating the fault-free behavior of a given state of the approximate system, are constructed. The choice of actuator locations ensures that the residual of each filter is sensitive to faults in only one actuator and decoupled from the rest, thus, allowing complete fault isolation. Finally, a set of switching rules are derived to orchestrate switching from the faulty actuators to healthy fall-backs in a way that preserves closed-loop stability and minimizes the closed-loop performance deterioration resulting from actuator faults. Precise FDI thresholds and control reconfiguration criteria that account for model reduction errors are derived to prevent false alarms when the reduced order model-based fault-tolerant control structure is implemented on the process. A singular perturbation formulation is used to link these thresholds with the degree of separation between the slow and fast eigenvalues of the spatial differential operator. The developed methodology is successfully applied to the problem of constrained, actuator fault-tolerant stabilization of an unstable steady-state of a representative diffusion-reaction process. © 2007 American Institute of Chemical Engineers *AIChE J*, 53: 1518–1537, 2007

Keywords: partial-differential equations, model reduction, fault detection and isolation, residual generation, nonlinear control, actuator constraints, stability region, actuator reconfiguration, singular perturbations, transport-reaction processes

Introduction

One of the central problems at the interface of process control and operations is the development of systematic methods for the diagnosis and handling of faults. The motivation for studying this problem stems in part from the vulnerability of automated industrial processes to faults (for example, malfunctions in control actuators, measurement sensors and process equipment), as well as the increased emphasis placed on safety, reliability and profitability in the operation of industrial processes. It is well known that faults can lead to serious degradation in the system performance, and

Correspondence concerning this article should be addressed to N. H. El-Farra at nhelfarra@ucdavis.edu.

may even lead to a complete breakdown of process operation, if not handled properly in the control system design. In this light, it is only natural that the subjects of fault diagnosis and fault-tolerant control (FTC) have become the focus of considerable research interest over the past few decades in both the academic and industrial circles (for example, see[1,2,3] and the references therein).

The main aims of fault-tolerant control are to preserve the integrity of the process, ensure satisfaction of the operational objectives after the appearance of a fault (possibly after a short period of degraded performance), and prevent a fault from causing a failure at the system level. Achieving these objectives requires the integration of two important tasks in the design and implementation of the fault-tolerant control system. The first task is fault diagnosis, that is, the detection and identification of faults with sufficient accuracy on the basis of which corrective action can be taken. The literature on fault diagnosis is quite extensive and covers both statistical and pattern recognition-based approaches (for example,[4,5,6,7,8,9,10]), as well as model-based approaches (for example,[11,12,13,14,15,16,17,18,19]). Once the faults have been detected and identified, the second task is that of fault compensation, which is typically accomplished through reconfiguration of the control system to cancel the effects of the faults or to attenuate them to an acceptable level (for example,[20,21]). Approaches that combine on-line fault diagnosis and control system reconfiguration to deal with faults are usually referred to as active fault-tolerant control systems. Other approaches that have been pursued for the design of fault-tolerant control systems include passivity-based methods, which do not involve fault diagnosis, and rely mainly on robust control techniques to enforce fault-tolerance without altering the control structure (for example,[22,23]).

Despite the substantial and growing body of literature on the problem of fault diagnosis, most of the research work in this area has focused on spatially homogeneous processes modeled by systems of ordinary differential equations. There are many examples in the process industries, however, where the overall process dynamics are characterized by spatial variations owing to underlying physical phenomena, such as diffusion, convection, and phase-dispersion. A prime example are transport-reaction processes which permeate both traditional (for example, catalytic packed-bed reactors) and developing industries (for example, chemical vapor deposition of thin films for microelectronics manufacturing, aerosol-based production of nanoparticles used in medical applications). The control problem arising in the context of transport-reaction processes often involves the regulation of spatially distributed variables (such as temperature and concentration spatial profiles) using spatially-distributed control actuators and measurement sensors. Many transport-reaction processes are also naturally modeled by highly dissipative partial differential equation (PDE) systems, such as parabolic PDE systems, whose dominant dynamics can be captured by finite-dimensional systems owing to a characteristic separation property that partitions the eigenspectrum of the spatial differential operator into a finite slow set and an infinite stable fast complement.[24,25]

Over the past decade, the subject of distributed parameter systems has evolved into an active area within process control research. Examples include results on source identification,[26] low-order nonlinear and robust control using approximate inertial manifolds,[27,28] distributed controller design using generalized invariants,[29] passivity and thermodynamics-based control,[30,31] low-order control-relevant modeling,[32] input constrained,[33] and predictive[34] control of parabolic PDE systems, state observation and adaptive control,[35] and optimal actuator placement.[36] Compared with these efforts and many others in this area, the problem of designing integrated fault diagnosis and fault-tolerant control systems for distributed processes has received limited attention. For mechanical and aerospace engineering systems, a number of research efforts have studied aspects of the fault detection (for example,[37,38]) and control reconfiguration problems (for example,[39,40]). The majority of existing results, however, have been developed on the basis of approximate linear models of the distributed parameter system and without taking complexities, such as nonlinearities, control constraints and limited state measurements into account. In the area of process control, on the other hand, efforts to address the fault-tolerant control problem have focused mainly on the control reconfiguration aspects of the problem (for example,[41,42]), under the assumptions that the faults are known and that complete state measurements are available. An examination of the available literature at this stage reveals the lack of a unified framework for the design of integrated fault diagnosis and fault-tolerant control systems for nonlinear distributed processes. This in turn limits the achievable control quality and reliability in the operation of transport-reaction processes.

Motivated by these considerations, we developed in[43] a hierarchical fault-tolerant control architecture for spatially distributed processes described by nonlinear parabolic PDEs with control constraints and control actuator faults. The architecture integrates model-based fault detection, spatially distributed feedback and supervisory control on the basis of appropriate reduced-order models that capture the dominant dynamics of the distributed process. Appropriate fault detection thresholds and controller reconfiguration criteria were derived for the implementation of the fault-tolerant control architecture on the distributed system. Given that the diagnostic filter is designed to only detect faults, a residual exceeding the specified threshold indicates that some fault has occurred in one or more actuators of the active control configuration, but does not pinpoint the location of the fault. This necessitates that the supervisor shut down all the actuators of the current configuration upon fault detection, including possibly healthy actuators, and switch to an appropriate fall-back configuration whose entire set of actuators are well functioning to ensure fault-tolerance. To avoid the unnecessary shut down of healthy actuators, a fault isolation scheme that identifies the faulty actuators within the active set needs to be incorporated into the fault-tolerant control architecture. The ability to distinguish between faults in different actuators depends to a large extent on the structure of the input operator, which describes the channels through which the different actuators affect the process evolution. For spatially distributed processes, this structure depends on the actuator locations which provide the designer with an additional degree of freedom that can be exploited to guide the design of an easy-to-implement fault isolation scheme. Furthermore, since the reconfiguration logic developed in[43] focuses only on closed-loop stability, additional performance objectives need to be incorporated in the selection of the fallback actuators to ensure not only stability, but also minimal performance deterioration upon actuator switching.

In this work, we present a methodology for the design of integrated, model-based fault diagnosis and fault-tolerant control (FTC) systems for transport-reaction processes, modeled by nonlinear parabolic PDEs with control constraints and actuator faults. The methodology brings together feedback control, fault detection and isolation (FDI), and performance-based supervisory switching between multiple actuator configurations. Initially, model reduction techniques are used to obtain an approximate, finite-dimensional system that captures the dominant dynamic characteristics of the PDE system. The approximate model is used to synthesize, for each actuator configuration, a stabilizing nonlinear feedback controller, and characterize its stability region in terms of the control constraints and actuator locations. The actuator locations are then chosen, such that the evolution of each dominant mode, in some transformed coordinates, is excited by only one actuator and decoupled from the rest. Next, a set of dedicated modal filters, each replicating the fault-free behavior of a given mode using measurements of the other modes, is constructed, and the discrepancy between the evolution of the fault-free and actual modes are used as residuals. The specific way in which the actuators influence each mode ensures that the residual of each filter is sensitive to faults in only one actuator, and can, therefore, be used to discern the fault or health status of that actuator at any given time. Following FDI, a set of switching laws are derived to orchestrate switching from the faulty actuators to healthy fallbacks in a way that preserves closed-loop stability, and minimizes the closed-loop performance deterioration resulting from actuator faults and subsequent actuator switching. Owing to the inherent approximation errors in the reduced-order model, appropriate FDI and control reconfiguration criteria are derived for the implementation of the fault-tolerant control structure on the process to prevent false alarms. Using singular perturbations, the criteria is expressed in terms of residual thresholds that capture the expected size of each residual in the absence of faults in its dedicated actuator, and is linked to the extent of separation between the slow and fast eigenvalues of the spatial differential operator. Finally, the integrated control, FDI and reconfiguration methodology is applied to the problem of actuator fault-tolerant stabilization of an unstable steady-state of a diffusion-reaction process.

Preliminaries

Scope

We consider transport-reaction processes modeled by nonlinear parabolic PDEs of the form

$$\frac{\partial \bar{x}}{\partial t} = \alpha\frac{\partial^2 \bar{x}}{\partial z^2} + \beta\frac{\partial \bar{x}}{\partial z} + f(\bar{x}) + \omega\sum_{i=1}^{l} b_i^{k(t)}(z)[u_i^{k(t)}(t) + f_{a_i}^{k(t)}(t)] \quad (1)$$

$$-u_{i,\max}^k \le u_i^{k(t)}(t) \le u_{i,\max}^k, \quad i \in \mathcal{I}, \quad k(t) \in \mathcal{K} \quad (2)$$

$$\mathcal{I} := \{1,2,...,l\}, \ \mathcal{K} := \{1,2,...,N\}, \ l,N < \infty \quad (3)$$

subject to the boundary and initial conditions

$$c_i\bar{x}(\eta_i,t) + d_i\frac{\partial \bar{x}}{\partial z}(\eta_i,t) = 0, \quad i = 1,2, \quad \bar{x}(z,0) = \bar{x}_0(z) \quad (4)$$

where $\bar{x}(z, t) \in \mathbb{R}$ denotes the state variable, $z \in [\eta_1, \eta_2] \subset \mathbb{R}$ is the spatial coordinate, $t \in [0, \infty)$ is the time, $f(\bar{x})$ is a nonlinear function, u_i^k is the i-th manipulated input (control actuator) associated with the k-th control configuration, $u_{i,\max}^k$ is a positive real number that captures the size of the constraints on the i-th actuator of the k-th control configuration, $f_{a_i}^k \in \mathbb{R}$ denotes a fault in the i-th control actuator of the k-th control configuration, and $k(t)$ is a discrete variable that takes values in a finite set $\mathcal{K}$, and denotes which control configuration is active at any given time. The coefficients α, β, ω, c_i, d_i, are constants with $\alpha > 0$, and $\bar{x}_0(z)$ is a smooth function of z. The function $b_i^k(z) \in L_2(\eta_1, \eta_2)$ is a square integrable function of z that describes how the control action $u_i^k(t)$, is distributed in the interval $[\eta_1, \eta_2]$. Throughout this article, the notations $|\cdot|$, $\|\cdot\|$ and $\|\cdot\|_2$ will be used to denote the standard Euclidean norm, the L_2 norm associated with a finite-dimensional Hilbert space, and the L_2 norm associated with an infinite-dimensional Hilbert space, respectively. The order of magnitude notation $O(\varepsilon)$ will also be used. In particular, $\delta(\varepsilon) = O(\varepsilon)$ if there exist positive real numbers, k_1 and k_2, such that $|\delta(\varepsilon)| \le k_1|\varepsilon|$, $\forall\ |\varepsilon| \le k_2$. Finally, the notation $x(T^+)$ denotes the limit of the trajectory $x(t)$, as T is approached from the right, that is, $x(T^+) = \lim_{t \to T^+} x(t)$.

Introducing the infinite-dimensional state space $\mathcal{H} = L_2(\eta_1, \eta_2)$, with inner product and norm

$$(\omega_1,\omega_2) = \int_{\eta_1}^{\eta_2} \omega_1(z)\omega_2(z)\sigma(z)dz, \ \ \|\omega_1\|_2 = (\omega_1,\omega_1)^{\frac{1}{2}} \quad (5)$$

where ω_1, ω_2 are two elements of $L_2(\eta_1, \eta_2)$, and σ is an appropriate weighting function, the PDE of Eqs. 1–4 can be formulated as an infinite-dimensional system of the form

$$\dot{x} = \mathcal{A}x + \mathcal{B}^k(u^k + f_a^k) + f(x), \ \ x(0) = x_0 \quad (6)$$

where $x(t) = \bar{x}(z, t)$, $t > 0$, $\eta_1 < z < \eta_2$, is the state function defined on $\mathcal{H}$, $\mathcal{A}$ is the differential operator defined as

$$\mathcal{A}\phi = \alpha\frac{d^2\phi}{dz^2} + \beta\frac{d\phi}{dz}, \ \ \eta_1 < z < \eta_2$$

where $\phi(\cdot), \frac{d\phi}{dz}$ are absolutely continuous on (η_1, η_2), with the following dense domain

$$D(\mathcal{A}) = \left\{\phi \in L_2(\eta_1,\eta_2) : \mathcal{A}\phi \in L_2(\eta_1,\eta_2), \right.$$
$$\left. c_i\phi(\eta_i) + d_i\frac{d\phi}{dz}(\eta_i) = 0, i = 1,2\right\}$$

$\mathcal{B}^k$ is the input operator defined as

$$\mathcal{B}^k(u^k + f_a^k) = \omega\sum_{i=1}^{l} b_i^k(\cdot)[u_i^k + f_{a_i}^k]$$

where $u^k = [u_1^k\ u_2^k \cdots u_l^k]'$ and $f_a^k = [f_{a,1}^k f_{a,2}^k \cdots f_{a,1}^k]'$, $f(x(t)) = f(\bar{x}(z, t))$ is locally Lipschitz and satisfies $f(0) = 0$, and $x_0 = \bar{x}_0(z)$. For $\mathcal{A}$, the eigenvalue problem is defined as $\mathcal{A}\phi_j = \lambda_j\phi_j$, $j = 1,\ldots,\infty$, where λ_j denotes an eigenvalue, and ϕ_j denotes an eigenfunction. The eigenspectrum of $\mathcal{A}$, denoted by $\sigma(\mathcal{A})$, is defined as the set of all eigenvalues of $\mathcal{A}$, that is, $\sigma(\mathcal{A}) = \{\lambda_1, \lambda_2, \ldots\}$. For highly-dissipative PDE systems, the eigenspectrum of $\mathcal{A}$ can be partitioned into a finite part consisting of m slow eigenvalues, and a stable infinite complement containing the remaining fast eigenvalues, and the separation between the slow and fast eigenvalues of $\mathcal{A}$ is large. These properties are stated precisely in Assumption 1,[44] and are satisfied by the majority of diffusion-convection-reaction processes.[24,25,28]

Assumption 1:

1. *$Re\{\lambda_1\} \geq Re\{\lambda_2\} \geq \cdots \geq Re\{\lambda_j\} \geq \cdots$, where $Re\{\lambda_j\}$ denotes the real part of λ_j.*

2. *$\sigma(\mathcal{A})$ can be partitioned as $\sigma(\mathcal{A}) = \sigma_1(\mathcal{A}) + \sigma_2(\mathcal{A})$, where $\sigma_1(\mathcal{A})$ consists of the first m (with m finite) eigenvalues, that is, $\sigma_1(\mathcal{A}) = \{\lambda_1, \ldots, \lambda_m\}$, and $\frac{|Re\{\lambda_1\}|}{|Re\{\lambda_m\}|} = O(1)$.*

3. *$Re\{\lambda_{m+1}\} < 0$ and $\frac{|Re\{\lambda_m\}|}{|Re\{\lambda_{m+1}\}|} = O(\varepsilon)$ where $\varepsilon < 1$ is a small positive number.*

Problem formulation and solution methodology

Consider the system of Eqs. 1–4 (and its abstract evolution equation in Eq. 6), for which N distinct control actuator configurations are available for possible use in feedback control. Each control configuration consists of l constrained control actuators placed at different locations, ξ_i^k, $i = 1,..., l$, across the spatial domain. The vector of actuator locations in the k-th configuration will be denoted by $\xi^k = [\xi_1^k \; \xi_2^k \; \cdots \; \xi_l^k]'$. While a given actuator may belong to more than one control configuration, no two control configurations share the same exact set of actuators. At any given time, only one actuator configuration is to be active for control, while the rest are kept dormant. We assume that operation starts using a given control configuration, and that, at some unknown time, a fault occurs in one or more actuators in this configuration. We also assume that direct measurements of the manipulated inputs are not available. The problems under consideration include how to detect that a fault has occurred, how to identify the faulty actuators in the operating configuration, and how to determine which of the available fallback actuator configurations should be activated to maintain closed-loop stability and minimize the deterioration in the process performance. To address these problems, we formulate the following objectives:
1. Initially, model reduction techniques are employed to derive a finite-dimensional system that captures the dominant dynamic characteristics of the infinite-dimensional system of Eq. 6.
2. Then, the approximate finite-dimensional system is used to synthesize, for each control configuration, a stabilizing nonlinear feedback controller that accounts for actuator constraints, and explicitly characterize its constrained stability region.
3. Next, a set of dedicated FDI filters that replicate the fault-free behavior of the approximate finite-dimensional closed-loop system are designed. Appropriate FDI thresholds are derived, using singular perturbation techniques, to discriminate between faults and approximation errors.
4. Finally, switching laws are devised to orchestrate the transition from the faulty actuators to well-functioning fallbacks in a way that respects the control constraints, maintains closed-loop stability and minimizes closed-loop performance losses.

Illustrative example: a diffusion-reaction process

In this section, we introduce a diffusion-reaction process example that will be used throughout the article to illustrate the design and implementation of the fault diagnosis and fault-tolerant control strategies to be presented in the next two sections. To this end, consider a long, thin catalytic rod in a reactor. The reactor is fed with pure species A, and a zeroth-order exothermic reaction of the form $A \rightarrow B$ takes place on the rod. Since the reaction is exothermic, a cooling medium in contact with the rod is used for cooling. Under standard modeling assumptions, the spatiotemporal evolution of the dimensionless rod temperature is described by the following parabolic PDE

$$\frac{\partial \bar{x}}{\partial t} = \frac{\partial^2 \bar{x}}{\partial z^2} + \beta_T \exp\left(-\frac{\gamma}{1+\bar{x}}\right) + \beta_U\left(\sum_{i=1}^{l} b_i(z)[u_i(t) + f_{a_i}(t)] - \bar{x}\right) - \beta_T e^{-\gamma} \qquad (7)$$

subject to the boundary and initial conditions

$$\bar{x}(0,t) = 0, \;\; \bar{x}(\pi,t) = 0, \;\; \bar{x}(z,0) = \bar{x}_0(z) \qquad (8)$$

where $\bar{x}$ denotes the dimensionless rod temperature, β_T denotes a dimensionless heat of reaction, γ denotes a dimensionless activation energy, β_U denotes a dimensionless heat transfer coefficient, $u_i(t)$ denotes the i-th manipulated input, $f_{a_i}(t)$ denotes the fault in the i-th actuator, and $b_i(z)$ denotes the i-th actuator distribution function. The following typical values of the process parameters are used: $\beta_T = 50.0$, $\beta_U = 2.0$, $\gamma = 2.0$.

For these values, it can be verified that the operating steady-state $\bar{x}(z,t) = 0$ is unstable (the linearized model around the zero steady-state has three positive eigenvalues). The control objective is to stabilize the rod temperature profile at this unstable, spatially-uniform steady-state by manipulating the temperature of the cooling medium in the presence of actuator constraints and faults. To achieve this objective, a total of six-point actuators ($\xi_A = \pi/2$, $u^A_{\max} = 1.5$), ($\xi_B = \pi/3$, $u^B_{\max} = 1.7$), ($\xi_C = \pi/6$, $u^C_{\max} = 1.7$), ($\xi_D = 3\pi/4$, $u^D_{\max} = 4.0$), ($\xi_{\mathrm{E}} = 2\pi/3$, $u^E_{\max} = 4.2$), ($\xi_F = \pi/16$, $u^F_{\max} = 1.0$), are assumed to be available. Only three actuators, however, are to be active at any given time, while the other three are kept dormant. We assume that operation starts using actuators (A, B, C), and that at some unknown time, a fault occurs in one or more actuators in this configuration. The problems under consideration include how to detect that a fault has occurred in the operating configuration, how to identify the faulty actuators, and how to determine which of the fallback actuators (D, E, F) should be activated to maintain closed-loop stability and minimize the deterioration in the process performance.

In the next section, we begin to address the problem by applying Galerkin's method to the system of Eq. 6 and deriving an approximate finite-dimensional system to be used as the basis for the design of the fault diagnosis and fault-tolerant control architecture.

Derivation of a Reduced-Order Model

Let $\mathcal{H}_s$, $\mathcal{H}_f$ be modal subspaces of the operator $\mathcal{A}$, defined as $\mathcal{H}_s = \text{span}\{\phi_1, \; \phi_2, \ldots, \phi_m\}$ and $\mathcal{H}_f = \text{span}\{\phi_{m+1}, \phi_{m+2}, \ldots\}$ (the existence of $\mathcal{H}_s$, $\mathcal{H}_f$ follows from Assumption 1). 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 x of the system of Eq. 6 can be decomposed as $x = x_s + x_f = \mathcal{P}_s x + \mathcal{P}_f x$. Applying $\mathcal{P}_s$ and $\mathcal{P}_f$ to the system of Eq. 6, and using the earlier decomposition for x, the system of Eq. 6 can be rewritten in the following equivalent form

$$\frac{dx_s}{dt} = \mathcal{A}_s x_s + \mathcal{B}_s^k(u^k + f_a^k) + f_s(x_s, x_f), \;\; x_s(0) = \mathcal{P}_s x_0 \quad (9)$$

$$\frac{dx_f}{dt} = \mathcal{A}_f x_f + \mathcal{B}_f^k(u^k + f_a^k) + f_f(x_s, x_f), \;\; x_f(0) = \mathcal{P}_f x_0 \quad (10)$$

where $\mathcal{A}_s = \mathcal{P}_s\mathcal{A}$, $\mathcal{B}_s = \mathcal{P}_s\mathcal{B}$, $f_s = \mathcal{P}_s f$, $\mathcal{A}_f = \mathcal{P}_f\mathcal{A}$, $\mathcal{B}_f = \mathcal{P}_f\mathcal{B}$, and $f_f = \mathcal{P}_f f$. In Eq 9, $\mathcal{A}_s$ is a diagonal matrix of dimension $m \times m$ of the form $\mathcal{A}_s = diag\{\lambda_j\}$, $f_s(x_s, x_f)$ and $f_f(x_s, x_f)$ are Lipschitz nonlinear functions, and $\mathcal{A}_f$ is an unbounded differential operator which is exponentially stable (following from Assumption 1, part 3, and the selection of $\mathcal{H}_s$, $\mathcal{H}_f$). In the remainder of this article, we will refer to the systems of Eqs. 9–10 as the slow and fast subsystems, respectively. Neglecting the fast and stable infinite-dimensional x_f-subsystem of Eq. 10, the following approximate, m-dimensional slow system is obtained

$$\frac{d\bar{x}_s}{dt} = \mathcal{A}_s\bar{x}_s + \mathcal{B}_s^k(u^k + f_a^k) + f_s(\bar{x}_s, 0) \quad (11)$$

where the bar symbol in $\bar{x}_s$ denotes that these variables are associated with a finite-dimensional system. The system of Eq. 11 will be referred to as the reduced system.

In the next two sections, we present an integrated FDI-FTC architecture that brings together fault detection, isolation and control actuator reconfiguration to address the objectives outlined in the problem formulation subsection. To highlight the main features of this architecture, we begin in the next section by discussing the design methodology of the main components of the FDI-FTC architecture on the basis of the finite-dimensional approximate model of Eq. 11. We then turn in the following section to address the practical implementation issues that arise when the FDI-FTC architecture is implemented on the infinite-dimensional system of Eq. 6. To simplify the presentation of our results, we will consider only the state feedback control problem where the state, $\bar{x}(z, t)$, is assumed to be available for measurement at all locations, $z \in [\eta_1, \eta_2]$, and for all times. Results on the output feedback control problem can be found in.[45]

Integrated FDI-FTC Structure using the Reduced-Order Model

The main components of the FDI-FTC architecture include the feedback controllers, the FDI filters and a high-level supervisor. Following is a discussion of how each component is designed on the basis of the reduced-order model of Eq. 11 that approximates the dominant dynamics of the infinite-dimensional system of Eq. 6.

Feedback controller synthesis

Referring to the system of Eq. 11, the objectives of this step are to: (a) synthesize, for each actuator configuration, a stabilizing feedback controller that respects the control constraints, and (b) explicitly characterize the stability region associated with each controller in terms of the constraints and the actuator locations. There are several controller design methods that can be used to meet these objectives (for example,[33,46,47]). For the sake of generality, we will not limit the discussion to any particular controller design method. Instead, we will assume that the desired controllers have already been synthesized, and their stability regions explicitly characterized (see [41] and the simulation example at the end of this section for how to obtain explicit expressions for the controllers and their stability regions).

Assumption 2: *For each $k \in \mathcal{K}$, there exist: (1) bounded feedback control laws of the general form*

$$u_i^k = p_i(\bar{x}_s, u_{i,\max}^k, \xi^k), \;\; i = 1, ..., l \quad (12)$$

where $p_i(\cdot)$ is a nonlinear function and ξ^k is the vector denoting the spatial placement of the control actuators, and (2) a set $\bar{\Omega}_s^k(u_{\max}^k, \xi^k)$: $= \{\bar{x}_s \in \mathcal{H}_s : \|\bar{x}_s\| \leq \delta_s\}$ such that $|u_i^k| \leq u_{i,\max}^k$ for all $\bar{x}_s \in \bar{\Omega}_s^k(u_{\max}^{\mathrm{k}}, \xi^k)$ and the origin of the closed-loop system of Eqs. 11–12 is exponentially stable for all $\bar{x}_s$ $(0) \in \bar{\Omega}_s^k(u_{\max}^k, \xi^k)$, where $p(\cdot) = [p_1(\cdot)\ p_2(\cdot) \cdots p_l(\cdot)]'$ and $u_{\max}^k = [u_{1,\max}^k\ u_{2,\max}^k \cdots u_{1,\max}^k]'$.

Remark 1: Note that the feedback control laws for the different actuator configurations share the same structure, and differ only in where the control action is applied. Furthermore, owing to the dependence of the control action on the actuator locations, the presence of control constraints imposes fundamental limitations on where the actuators can be placed to achieve stabilization from a given initial condition. For a given initial condition, $\bar{\Omega}_s^k$ characterizes the set of admissible actuator locations. Alternatively, for a fixed actuator location, $\bar{\Omega}_s^k$ describes the feasible initial conditions. Knowledge of the feasible initial conditions and actuator locations is necessary not only for stabilization under a given control configuration, but also for the design of the control actuator reconfiguration logic that needs to be implemented by the supervisor in the event of faults (see the subsection on stability and performance-based actuator reconfiguration).

Design of dedicated fault detection and isolation filters

The ability to distinguish between faults in different actuators depends to a large extent on the structure of the input operator which determines the channels through which the different actuators affect the evolution of the states. For spatially distributed processes, this structure depends on the spatial locations of the actuators, which provide the designer with an additional degree of freedom that can be exploited to guide the design of an easy-to-implement fault isolation scheme.

The central idea behind the FDI scheme presented here is to select the actuator locations in a manner that gives the input operator a specific structure that lends itself to easy fault isolation via a bank of dedicated FDI filters. Specifically, the actuator locations are chosen such that the evolution of each slow mode, in appropriately chosen transformed coordinates, is excited by only one actuator, and is decoupled from the rest. A filter can then be designed for each mode such that its residual is sensitive to only one actuator. This allows for complete fault isolation. In order to illustrate the main idea behind the design of the FDI filters, we will impose the following assumption on the system of Eq. 11 (see Remark 6 for a discussion on how this assumption can be relaxed).

Assumption 3: *$\ell = m$ and the inverse of the input operator, $\mathcal{B}_s^{-1}$, exists.*

The requirement that $\ell = m$, which is met by having the number of actuators equal to the number of slow modes, ensures that the reduced-order system of Eq. 11 has as many states as it has manipulated inputs (that is, has a square structure). This, together with an appropriate selection of the actuator locations, ensures the existence of the inverse input operator $\mathcal{B}_s^{-1}$. The invertibility of the input operator, in turn, guarantees the existence of an invertible, bounded operator $\mathcal{T}_s^k$ such that $\mathcal{T}_s^k\, \mathcal{B}_s^k = \mathcal{D}_s^k$, where $\mathcal{D}_s^k$ is a diagonal operator. For simplicity, and without loss of generality, we will choose $\mathcal{D}_s^k$ to be the identity operator on $\mathcal{H}_s$. Consider now the transformation $\bar{v}_s = \mathcal{T}_s^k\, \bar{x}_s$, which transforms the approximate system of Eq. 11 into the following form

$$\begin{aligned}\frac{d\bar{v}_s}{dt} &= \mathcal{A}_s \mathcal{T}_s^{k^{-1}} \bar{v}_s + \mathcal{T}_s^k \mathcal{B}_s^k (u^k + f_a^k) + f_s(\mathcal{T}_s^{k^{-1}} \bar{v}_s, 0) \\ &:= \bar{f}_s(\bar{v}_s) + \mathcal{D}_s^k (u^k + f_a^k) \qquad (13)\end{aligned}$$

where $\bar{f}_s\ (\bar{v}_s) = \mathcal{A}_s \mathcal{T}_s^{k^{-1}} \bar{v}_s + f_s\ (\mathcal{T}_s^{k^{-1}} \bar{v}_s,\ 0)$. We will refer to the system of Eq. 13 as the transformed reduced system. To reveal the specific structure that this system possesses, we can further decompose the transformed approximate slow state $\bar{v}_s\ (t)$ as

$$\bar{v}_s(t) = \bar{v}_{s_1}(t) + \bar{v}_{s_2}(t) + \cdots + \bar{v}_{s_m}(t) \qquad (14)$$

where $\bar{v}_{s_i}(t) := \mathcal{P}_{s_i} \bar{v}_s(t) \in \mathcal{H}_{s_i} = \text{span}\{\phi_i\}$, $i = 1, \ldots, m$, is the state of a one-dimensional (1-D) system, describing the evolution of the *i*-th transformed slow mode, and $\mathcal{P}_{s_i}$ is the orthogonal projection operator that projects $\bar{v}_s(t) \in \mathcal{H}_s$ onto $\bar{v}_{s_i} \in \mathcal{H}_{s_i}$. Using this decomposition, the system of Eq. 13 can be written as

$$\frac{d\bar{v}_{s_i}}{dt} = \bar{f}_{s_i}(\bar{v}_s) + \mathcal{D}_{s_i}^k (u^k + f_a^k), \quad i = 1, 2, \ldots, m \qquad (15)$$

where $\mathcal{D}_{s_i}^k = \mathcal{P}_{s_i} \mathcal{T}_s^k\, \mathcal{B}_s^k = \mathcal{P}_{s_i} \mathcal{T}_s^k\, \mathcal{P}_s \mathcal{B}^k, \bar{f}_{s_i} = \mathcal{P}_{s_i} \bar{f}_s$. Using the definition of $\mathcal{D}_{s_i}^k$ and recalling that $\mathcal{B}^k u^k = \sum_{i=1}^m b_i^k(z) u_i^k$, the evolution equation for the *i*-th transformed slow mode can be written as

$$\begin{aligned}\frac{d\bar{v}_{s_i}}{dt} &= \bar{f}_{s_i}(\bar{v}_s) + \mathcal{P}_{s_i} \mathcal{T}_s^k \mathcal{P}_s \sum_{j=1}^m b_j^k(z)[u_j^k + f_{a_j}^k] \\ &= \bar{f}_{s_i}(\bar{v}_s) + \mathcal{P}_{s_i} \mathcal{T}_s^k \mathcal{P}_s b_i^k(z)[u_i^k + f_{a_i}^k] \qquad (16)\end{aligned}$$

for $i = 1, \ldots, m$, where we have used the fact that $\mathcal{P}_{s_i} \mathcal{T}_s^k \mathcal{P}_s b_j^k(z) = 0$ for $j \neq i$ due to the diagonal structure of the operator $\mathcal{T}_s^k \mathcal{B}_s^k$. Actuator FDI in the reduced system of Eq. 11 can now be accomplished by constructing the following set of dedicated FDI filters

$$\begin{aligned}&\frac{d\bar{w}_i}{dt} = \bar{f}_{s_i}(\bar{w}_i, [\bar{v}_s]^i) + \mathcal{P}_{s_i} \mathcal{T}_s^k \mathcal{P}_s b_i^k(z) p_i(\bar{w}_i, [\bar{v}_s]^i, u_{i,\max}^k, \xi^k), \\ &\bar{r}_i(t) = \|\bar{w}_i(t) - \bar{v}_{s_i}(t)\| \qquad (17)\end{aligned}$$

for $i = 1, \ldots, m$, where $\bar{w}_i \in \mathcal{H}_{s_i}$ is the state of the *i*-th filter, $\bar{r}_i$ is the residual, and the notation $[\bar{v}_s]^i$ denotes the set of all transformed states except the *i*-th one, that is, $[\bar{v}_s]^i = \{\bar{v}_{s_j},\ j \neq i, j = 1, \ldots, m\}$. Proposition 1 formalizes the proposed FDI scheme and states its main properties. The proof of this proposition can be found in the Appendix.

Proposition 1: *Consider the approximate, finite-dimensional closed-loop system of Eqs. 11–12, for which Assumption 3 is satisfied, with $k(0) = j \in \mathcal{K}$. Consider also the systems of Eqs. 16–17 with $\bar{w}_i(0) = \bar{v}_{s_i}(0)$, $i = 1, \ldots, m$. Let $\overline{T}_{d_i}$ be such that $f_{a_i}^j(t) \equiv 0$ for all $0 \leq t < \overline{T}_{d_i}$, for all $i = 1, \ldots, m$. Then $\bar{r}_i(\overline{T}_{d_i}^+) > 0$ if and only if $f_{a_i}^j(\overline{T}_{d_i}) \neq 0$.*

Remark 2: Each filter in Eq. 17 provides an estimate of the expected closed-loop behavior of the *i*-th slow mode of the transformed reduced system in the absence of faults in the *i*-th actuator. Therefore, when the filter state is initialized at the same value as the corresponding mode (within the stability region of the active control configuration), the evolution of $\bar{w}_i(t)$ will be identical to $\bar{v}_{s_i}(t)$, and, hence, $\bar{r}_i(t) = 0$, in the absence of faults in the *i*-th actuator. This ensures that, for all times, the *i*-th residual is sensitive only to faults in the *i*-th actuator and not to initialization errors. In the presence of faults, the effect of the fault is registered by a change in the evolution of $\bar{v}_{s_i}$, but not in that of $\bar{w}_i$ (since the filter state dynamics include only the computed control action, u_i^k, and not the implemented control action, $(u_i^k + f_{a_i}^k)$. This change is detected by a nonzero value of $\bar{r}_i(t)$, and declared as a fault in the *i*-th actuator. Note that both partial and complete actuator failures can be detected and isolated in this manner.

Remark 3: The judicious selection of the locations of the control actuators to ensure the invertibility of the input operator $\mathcal{B}_s^k$, is critical to the development of the filter-based fault isolation scheme presented in Eq. 17. The invertibility (or pseudo-invertibility in the case of a nonsquare system-see Remark 6) of the input operator ensures modal controllability of all the dominant (slow) modes of the infinite-dimensional system. For a given mode, modal controllability is a measure of the total control authority of all actuators at the chosen locations over that mode (for example, see[36,48]). Zero modal controllability of a given mode, for a specific actuator spatial placement, implies that none of the controllers has any authority over that mode. Thus, invertibility of the input operator guarantees that the modal controllability for each mode is nonzero; that is, at least one controller has some authority over a given mode. This is also consistent with the notion of approximate controllability for the class of PDEs with Riesz-spectral operators.[49] Beyond modal (and approximate) controllability, invertibility of the input operator ensures that the different controllers exert their authority through linearly-independent channels. This in turn allows transforming the reduced system into the diagonal form of Eq. 16, which is more amenable to FDI designs. In the transformed form, each slow mode is directly excited by only one input (actuator), and, therefore, the evolution of the state of the *i*-th filter is driven by the *i*-th actuator only and decoupled from the rest of the actuators. Consequently, the residual of the *i*-th filter reflects the fault or health status of the *i*-th actuator only, and is insensitive to faults that may occur in the other actuators in the sense that it will return a zero value even if the other actuators are faulty, as long as the *i*-th actuator itself is well functioning. The end result is a set of *m* FDI filters whose residuals are dedicated to identifying faults in the different actuators. To determine the fault or health status of a given actuator, one needs to simply look at the residual of the filter driven by this actuator.

Remark 4: The result of Proposition 1 guarantees that a fault in a given actuator is detected and isolated as soon as it occurs in the reduced system. Timely FDI enhances the ability of the control system to recover from failures through control system reconfiguration. Note also that since each residual is dedicated to only one actuator, the FDI scheme allows the complete isolation of both single and multiple faults that may occur simultaneously in different actuators.

Remark 5: The FDI filters of Eq. 17 differ from the filter design presented in[43] in two important ways. First, each filter in Eq. 17 is driven by only one actuator and is, therefore, capable of both fault detection and isolation, while the filter in[43] is driven by all the actuators and, is thus, capable of fault detection only. Another important difference is the fact that the filter in[43] only simulates (starting from a given initial condition) the fault-free behavior of the reduced closed-loop system, and, thus, requires no knowledge of the evolution of the approximate slow modes for implementation. In contrast, each filter in Eq. 17 relies on measurements, not simulated values, of all but the i-th approximate slow mode to generate an estimate of the fault-free evolution of $\overline{w}_i$. The reason that the actual (in lieu of the simulated) behavior of the slow modes is needed in implementing the FDI scheme has to do with the coupling between the different modes brought about by the presence of the nonlinear terms, as well as the requirement that each filter be dedicated to a single input only. To understand this point, note that even though an actuator, say $j \neq i$, does not directly enter the evolution equation of the i-th slow mode, a fault in actuator j can still influence the i-th slow mode by influencing the j-th mode, which in turn influences i-th mode through the coupling terms $\bar{f}_{s_i}(\cdot)$ and $p_i(\cdot)$. By using measurements of the j-th mode in the i-th filter equation, we ensure that, even if there are faults in actuator j influencing the behavior of that mode, the (possibly faulty) evolution of mode j affects both $\overline{w}_i$, and the i-th slow mode in exactly the same way, thus, making the residual of the i-th filter insensitive to faults in all, but the i-th, actuator.

Remark 6: It should be noted that the requirements of Assumption 3 are only sufficient, and not necessary, to be able to construct the dedicated FDI filters of Eq. 17. As explained in Remark 3 previously, the main idea behind the FDI scheme is to first transform the reduced system into a diagonal form, where each state is driven by only one input. While such a transformation is most transparent under the conditions of Assumption 3, it is still possible to find such a transformation even if the reduced system has an unequal number of states and inputs, and the inverse of the input operator is undefined. To illustrate this point by means of a concrete example, one may conceptually think of the abstract input operator as a matrix, and consider the case where the reduced system has fewer inputs than it has states, that is $\ell < m$. If the input matrix has full column rank (which can be ensured by appropriate selection of the actuator locations), then it is possible to define the pseudo-inverse (or left inverse) of B_s as ${B_s}^+ = (B_s'\, B_s)^{-1} B_s'$, and then use the transformation matrix $T_s = B_s^+$ which, when applied to the reduced system, yields $T_s B_s = B_s^+ B_s = (B_s' B_s)^{-1} B_s' B_s = I$, and ensures that the input matrix of the transformed system is the identity matrix.

Stability and performance-based actuator reconfiguration

Having detected and isolated the faults in the operating control configuration, the supervisor needs to select and activate appropriate fallback actuators in place of the faulty ones. A primary requirement for the fallback actuator configuration is to preserve closed-loop stability. However, since changing the actuator locations alters the closed-loop performance obtained prior to the faults, it is desirable to incorporate a performance criterion in the control reconfiguration logic, whereby the supervisor chooses fallback actuators that not only preserve closed-loop stability but also minimize the deterioration in the closed-loop performance resulting from actuator failure and subsequent actuator switching. To this end, we consider, for each of the fallback actuator configurations, the following measure of performance deterioration based on the finite-dimensional approximate system of Eq. 11

$$\bar{J}_s(\xi^k) = \int_{\bar{T}_{d_i}}^{\infty} \big[(\overline{e}_s(t, \xi^k), \mathcal{Q}_s \overline{e}_s(t, \xi^k)) + \overline{e}_u^T(\overline{x}_s(t), \xi^k) R\, \overline{e}_u(\overline{x}_s(t), \xi^k) \big]\, dt \qquad (18)$$

where $\overline{T}_{d_i}$ is the time of fault detection, $\overline{e}_s(t) := \overline{x}_s(t;\, \overline{x}_s(\overline{T}_{d_i}),\, \xi^{k(\bar{T}_{d_i})}) - \overline{x}_s(t; \overline{x}_s(\overline{T}_{d_i}),\, \xi^{k(\bar{T}_{d_i})})$, *where* $\overline{x}_s\ (t;\, \overline{x}_s(\overline{T}_{d_i}),\, \xi^{k(\bar{T}_{d_i})})$, is the response of the approximate closed-loop system obtained under the fallback configuration $\xi^{k(\bar{T}_{d_i})}$, to be activated after fault detection, $\overline{x}_s(t;\, \overline{x}_s(\overline{T}_{d_i}),\, \xi^{k(\bar{T}_{d_i})}$, is the response of the approximate closed-loop system that would be obtained in the absence of faults in the operating control configuration, $\xi^{k(\bar{T}_d)}$, $\overline{e}_u(t) : = p(\overline{x}_s(t),\, u^k_{\max}\, \xi^{k(\bar{T}_{d_i})}) - p(\overline{x}(t)_s,\, u^k_{\max},\, \xi^{k(\bar{T}_d)})$ is the discrepancy between the two control actions, $\mathcal{Q}_s$ is a coercive operator, and R is a positive definite matrix. The cost functional of Eq. 18 imposes penalties on the deviation of the closed-loop response, and control action resulting from switching actuator locations. Selecting an actuator configuration that minimizes this cost to replace the faulty actuator configuration results in a post-fault closed-loop performance that best matches (from among the candidate fall-back configurations) the original (that is, pre-fault) closed-loop performance that would have been obtained in the absence of faults.

Theorem 1 that follows describes how the feedback control, FDI, and actuator reconfiguration tasks are integrated to ensure fault-tolerance in the closed-loop reduced system. The proof can be found in the Appendix.

Theorem 1: *Consider the approximate, finite-dimensional closed-loop system of Eqs. 11–12 with* $k(0) = j \in \mathcal{K}$ and $\bar{x}_s \in \bar{\Omega}_s^j\ (u^j_{max}\ \xi^j)$. *Consider also the systems of Eqs. 16–17 with* $\overline{w}_i(0) = \overline{v}_{s_i}(0)$. *Let* $\overline{T}_{d_i} := \min\{t : \overline{r}_i(t) > 0\}$ *for some* $i = 1, \ldots, m$. *Furthermore, let* $\mathcal{D} := \{v \neq j : \bar{x}_s(\bar{T}_{d_i}) \in \bar{\Omega}_s^v(u^v_{\max},\ \xi^v), \xi^v_a = \xi^j_a, a \neq i\}$ *and let* $\xi^\mu = \arg\min_{v \in \mathcal{D}} \bar{J}_s(\xi^v)$. *Then the switching rule given by*

$$k(t) = \begin{Bmatrix} j, & 0 \leq t < \bar{T}_{d_i} \\ \mu, & t \geq \bar{T}_{d_i} \end{Bmatrix} \qquad (19)$$

exponentially stabilizes the origin of the closed-loop system.

Remark 7: The result of Theorem 1 can be understood using the following step-wise algorithm:

• Initialize the closed-loop system of Eqs. 11–12 using the actuators of control configuration j and an initial condition, $\bar{x}_s(0)$, that belongs to its stability region, $\bar{\Omega}^j(u^j_{\max}\ \xi^j)$.• • Initialize the FDI filters of Eq. 17 at the same initial conditions for the transformed system of Eq. 16, $\overline{w}_i(0) = \bar{v}_{s_i}(0)$, $i = 1, \ldots, m$.

• Monitor the evolution of the reduced closed-loop system, $\bar{x}_s(t)$, and the FDI filters, $\overline{w}_i(t)$. At the earliest time that one or more filter returns a nonzero residual, a fault is declared by the supervisor in the corresponding actuator(s).

• At the time of FDI, the supervisor performs the following tasks:

– Determine, from among the $N - 1$ available dormant configurations, the set of fallback configurations $\mathcal{D}$, that: (1) share the same set of healthy actuators with the operating configuration j, and (2) whose stability regions contain $\bar{x}_s$ at the time of fault detection.

– For each configuration in the set $\mathcal{D}$, evaluate the cost-to-go of Eq. 18 to determine the configuration μ, that results in the least performance deterioration when activated.

• Finally, activate actuator configuration μ to preserve closed-loop stability and ensure fault-tolerance.

Remark 8: Owing to its dependence on the fault detection time (which is unknown prior to process startup), the cost-to-go of Eq. 18 cannot be computed *a priori*. It can only be evaluated on-line after the faults have been detected and isolated. This task can then be achieved by running fast simulations of the reduced closed-loop system under the different candidate fallback actuator configurations to compare their respective performances and choose the optimal configuration. While the online computations required to evaluate the costs may introduce delays between the time faults are detected and the time the actuators are re-configured, such delays can be minimized by: (1) using computationally-efficient simulation tools that require minimum computational time and allow for making a timely determination of the optimal fallback configuration, and (2) designing the fallback configurations in a way that enhances their robustness against actuator switching delays. The latter approach can be realized by enlarging the stability regions of the fallback configurations (through appropriate selection of $u^k_{\max}\ \xi^k$), so as to minimize the possibility of having the state escape the stability regions during the delay period, while the closed-loop system is evolving under the faulty actuators.

Remark 9: The actuator reconfiguration strategy described in Theorem 1 differs from the one proposed in[43] in two ways. The first is that it accounts not only for closed-loop stability but also accommodates performance considerations in the selection of the fallback configuration. The other important difference is that, owing to the added fault isolation capability built into the fault-tolerant control design presented here, it is no longer necessary for the supervisor to shut down all the actuators of the faulty configuration upon fault detection as was the case in[43] where the filters were designed to only detect faults. Instead, the supervisor can now identify the faulty actuators in a given configuration by examining the individual residuals and replace only the faulty actuators, while keeping the healthy actuators of the operating configuration active. This is the reason that Theorem 1 limits the search among all possible fallback configurations to ones that share the same set of healthy actuators with the faulty configuration ($\xi^v_a = \xi^j_a$, $a \neq i$).

Remark 10: The successful implementation of the actuator reconfiguration law (which is the mechanism that enforces fault-tolerance) requires knowledge of the stability regions (that is, the sets of stabilizing initial conditions) associated with the fallback actuator configurations. Since exact computation of the entire stability region for a constrained nonlinear control system is in general not possible, it is important to select methods that provide sufficiently large (that is, nonconservative) estimates of the stability regions in order to avoid limiting the operating regions where recovery from faults is possible. An estimate that does not capture the stability region very well may result in excluding possibly feasible points in the state space (from where fault-tolerance can be guaranteed), and, thus, exclude viable backup actuator configuration candidates leading to unnecessary shut down of the process. Examples of available methods for estimating the size of the stability region include constructive procedures, such as Zubov's method[50] and level-set methods using a combination of several control Lyapunov functions (see, for example,[51]).

Application to a reduced-order model of a diffusion-reaction process

In this section, we demonstrate how the theoretical results presented so far can be used to design an integrated FDI-FTC scheme for the diffusion-reaction process of Eqs. 7–8, on the basis of an appropriate reduced-order model that captures the dominant dynamics of the PDE. We also present computer simulations that illustrate the application of this scheme to the reduced-order model. The feasibility of implementing the reduced-order model based FDI-FTC scheme on a sufficiently high-order discretization of the PDE is analyzed in detail at the end of the next section.

To derive a finite-dimensional approximate model of the process, we first note that the linearization of the PDE of Eq. 7–8 around the spatially uniform steady-state, $\bar{x}(z,t) = 0$, possesses three unstable eigenvalues. Therefore, we consider the first three eigenvalues to be the dominant ones and use standard Galerkin's method to derive the following third-order model that describes the approximate temporal evolution of the amplitudes of the first three eigenmodes

$$\bar{a} = F(\bar{a}) + G(\xi)[u + f_a] \tag{20}$$

where $\bar{a} = [\bar{a}_1\ \bar{a}_2\ \bar{a}_3]'$, $u = [u_1\ u_2\ u_3]'$, $f_a = [f_{a1}\ f_{a2}\ f_{a3}]'$, $F(\cdot) = [F_1(\cdot)\ F_2(\cdot)\ F_3(\cdot)]'$, $F_i = \lambda_i\bar{a}_i + f_i(\bar{a})$, G is a matrix whose i-th row is of the form $\beta_U[\phi_i(\xi_A)\ \ \phi_i(\xi_B)\ \ \phi_i(\xi_C)]$, $\bar{x}_s(t) := \sum_{i=1}^{3} \bar{a}_i(t)\phi_i(\cdot)$, λ_i and ϕ_i are, respectively, the i-th eigenvalue and i-th eigenfunction of the spatial differential operator, which are obtained from the solution of the eigenvalue problem given by

$$\lambda_i = -i^2, \quad \phi_i(z) = \sqrt{\frac{2}{\pi}}\sin(iz), \quad i = 1, \ldots, \infty$$

The nonlinear function f_i is given by $f_i(\bar{a}) = (\tilde{f_i}(\bar{a}), \phi_i(z))$, where $\tilde{f_i}(\bar{a}) = -\beta_U\Sigma^3_{i=1}\bar{a}_i\phi_i(z) - \beta_T e^{-\gamma} + \beta_T\ \exp(-\gamma/(1 + \Sigma^3_{i=1}\ \bar{a}_i\phi_i(z)))$, $i = 1,2,3$.

The origin of the system of Eq. 20 with $u \equiv 0$ and $f_a \equiv 0$, is unstable, and the control objective is to stabilize it in the presence of control constraints and faults. To achieve this

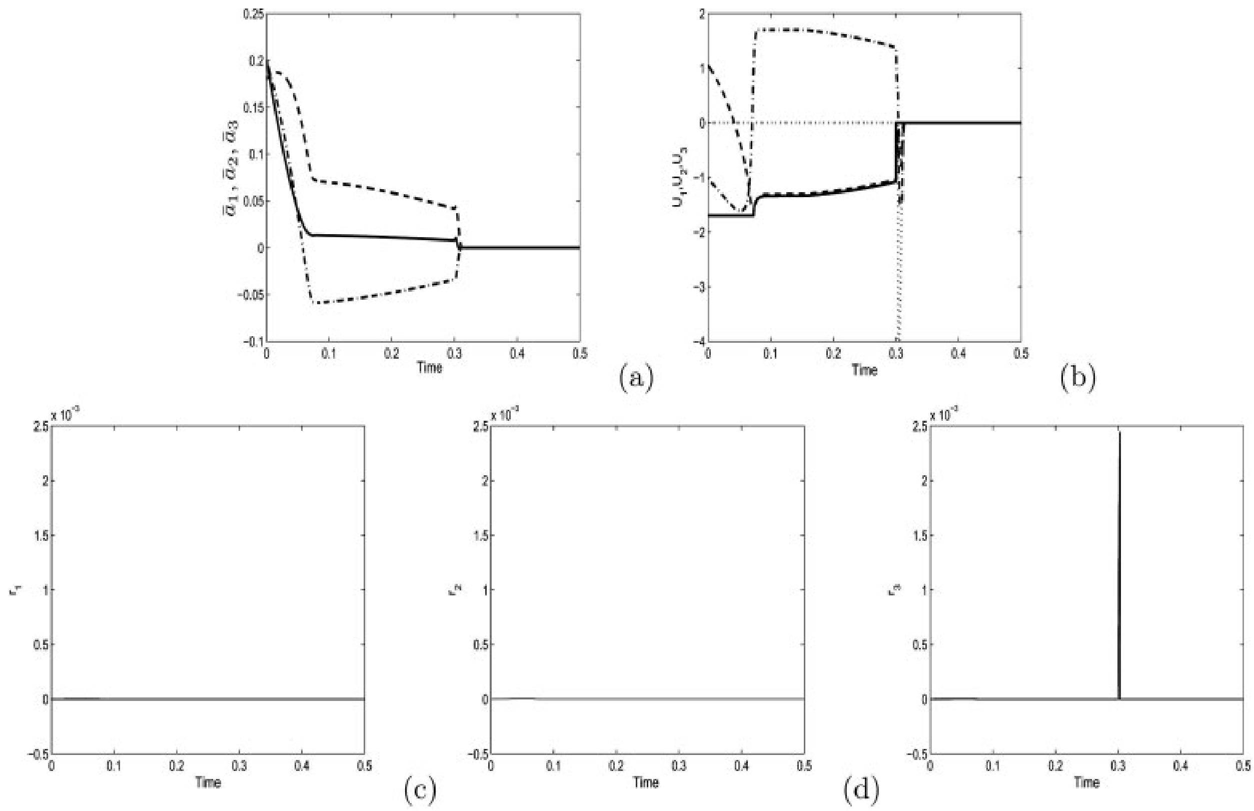

Figure 1. Evolution of: (a) the closed-loop states of the reduced-order system, (b) the manipulated inputs, and (c)–(e) the FDI filter residuals, when actuator *C* fails at $t = 0.3$, and actuator *D* is activated immediately.

The solid and dotted lines in (b) describe the manipulated input profiles for actuators *C* and *D*, respectively.

objective, we synthesize a bounded Lyapunov-based controller of the form

$$u = -\left(\frac{L_F^* V + \sqrt{(L_F^* V)^2 + (u_{\max}|(L_G V)'|)^4}}{|(L_G V)'|^2\left[1+\sqrt{1+(u_{\max}|(L_G V)'|)^2}\right]} \right)(L_G V)' \tag{21}$$

where $V = \bar{a}'P\bar{a}$ and

$$P = \begin{bmatrix} 20.4122 & 0.0723 & 0.3909 \\ 0.0723 & 30.973 & -5.1751 \\ 0.3909 & -5.1751 & 63.4094 \end{bmatrix}$$

is a positive-definite matrix, $L_F^* V = L_F V + \rho|\bar{a}|^2$, $L_F V = \sum_{i=1}^{3} \frac{\partial V}{\partial \bar{a}_i} F_i(\bar{a}_1, \bar{a}_2, \bar{a}_3)$ is the Lie-derivative of V along the vector field F, $\rho = 0.0001$, $L_G V = [L_{g_1}V \; L_{g_2}V \cdots L_{g_m}V]$, $L_{g_i}V = \sum_{j=1}^{3} \frac{\partial V}{\partial \bar{a}_j} g_{ij}$, and g_i is the i-th column of the matrix G. For a given choice of actuator locations and constraints, an estimate of the set of stabilizing initial conditions (stability region) is then obtained by constructing the invariant set: $\bar{\Omega}(u_{\max},\xi) = \{\bar{a} \in \mathbb{R}^3 : V(\bar{a}) \leq c_{\max}$ and $L_F^* V \leq u_{\max}|(L_G V)'|\}$, for some $c_{\max} > 0$ (see[33] for further details on the controller synthesis and the characterization of the stability region). It was verified that starting from the initial condition $\bar{a}(0) = [0.18 \; 0.2 \; 0.2]'$ (which belongs to the stability region of configuration (A, B, C)), the controller successfully stabilizes the states at the desired steady-state in the absence of faults. To design a set of dedicated FDI filters for the system of Eq. 20, we use the transformation $\bar{v} = G^{-1}(\xi)\bar{a}$ to obtain the following transformed system

$$\bar{v}_i \;=\; \chi_i(\bar{v}_1, \bar{v}_2, \bar{v}_3) + u_i(\bar{v}_1, \bar{v}_2, \bar{v}_3) + f_{a_i}, \quad i = 1,2,3 \tag{22}$$

where $\bar{v} = [\bar{v}_1 \; \bar{v}_2 \; \bar{v}_3]'$, $\chi(\cdot) = [\chi_1(\cdot) \; \chi_2(\cdot) \; \chi_3(\cdot)]' = G^{-1}F(G\bar{v})$. The explicit forms of the functions $\chi_i(\cdot)$, $i = 1, 2, 3$, are omitted for brevity. The FDI filters and their residuals are given by

$$\bar{w}_i \;=\; \chi_i(\bar{w}_i, [\bar{v}]^i) + u_i(\bar{w}_i, [\bar{v}]^i), \quad \bar{r}_i(t) = |\bar{w}_i(t) - \bar{v}_i(t)| \tag{23}$$

where $[\bar{v}]^i = \{\bar{v}_j, j = 1,2,3, j \neq i\}$. To demonstrate how the integrated FDI-FTC scheme works, we initialize the closed-loop system at $\bar{a}(0) = [0.18 \; 0.2 \; 0.2]'$ using actuator configuration (A,B,C), and initialize the filters at $\bar{w}_i(0) = \bar{v}_i(0)$, for $i = 1,2,3$. At $t = T_{f_1} = 0.3$, actuator C experiences total failure (see the solid line in Figure 1b). As shown in the residuals profiles in Figure 1c–1e this failure is detected and isolated immediately by the supervisor since it causes the residual dedicated to actuator C, r_3, to become nonzero at $T_{d_1} = 0.302$, while not affecting the other two residuals, thus, indicating that actuators A and B are healthy at that time. Notice that prior to the failure, all residuals have zero values and that, after FDI, the residuals are reinitialized (to allow FDI of possible future faults). Following FDI, the supervisor needs to decide which backup actuator (D, E, *or* F) is suitable for use in place of actuator C. By tracking the state over time, it was verified that $\bar{a}(T_{d_1})$ lies inside the stability regions of configurations (A, B, D) and (A, B, E), and outside the stability region of configuration (A, B, F). To decide which of the two feasible configurations (A, B, D) or (A, B, E) should be activated, Eq. 18 is used to evaluate and compare the costs incurred by implementing each configuration. The costs were found to be $\bar{J}_s = 1.823$ for configuration (A, B, E), and $\bar{J}_s = 1.684$ for configuration (A, B, D). Based on this finding, the supervisor activates actuator D to ensure both closed-loop stability and minimal deterioration in the closed-loop performance. The resulting closed-loop state and manipulated input profiles are shown in Figure 1a–1b.

Implementation of Integrated FDI-FTC Structure on the Infinite-Dimensional System

Having designed the various components of the FDI-FTC architecture on the basis of the reduced-order model, we proceed in this section to characterize how each component is implemented and the modifications that need to be made in order to ensure the desired stability and performance properties in the infinite-dimensional closed-loop system.

Feedback controller implementation

Proposition 2 that follows characterizes the stability properties of the state feedback controllers of Eq. 12 when implemented on the infinite-dimensional system of Eqs. 9–10. The proof, which relies on formulating the infinite-dimensional closed-loop system as a singularly perturbed system and analyzing its stability properties, is conceptually similar to the proof of Theorem 1 in[33] and is omitted for brevity.

Proposition 2: *Consider the system of Eqs. 9–10, for a fixed* $k \in \mathcal{K}$, *under the feedback control law* $u^k = p(x_s, u^k_{\max}, \xi^k)$, *where* $p(\cdot)$ *was defined in Assumption 2. Then given any* ${\delta_s}^k > 0$ *such that the set* $\Omega_s^k := \{x_s \in \mathcal{H}_s : \|x_s\| \le {\delta_s}^k\} \subset \bar{\Omega}_s^k$, *where* $\bar{\Omega}_s^k$ *was defined in Assumption 2, and given any* ${\delta_f}^k > 0$, *there exists a positive real number,* ε^*, *such that if* $\varepsilon \in (0, \varepsilon^*]$, $\|x_s(0)\| \le \delta_s^k$, *and* $\|x_f(0)\|_2 \le \delta_f^k$, *the origin of the closed-loop system is asymptotically (and locally exponentially) stable.*

Remark 11: Proposition 1 establishes that a controller that stabilizes the approximate slow system of Eq. 11 continues to enforce closed-loop stability for the infinite-dimensional system, provided that the separation between the slow and fast eigenvalues of the spatial differential operator is large enough. This separation property—characteristic of highly-dissipative PDEs—allows preserving the stability region associated with the reduced system in the sense that, for sufficiently small ε (that is, sufficiently large separation), the discrepancy between the stability region of the slow subsystem of Eq. 9, Ω_s^k, and the stability region of the reduced system of Eq. 11, $\bar{\Omega}_s^k$, can be made arbitrarily small. This result is important because it provides the needed theoretical justification for designing the feedback controllers and computing their stability regions on the basis of the approximate, finite-dimensional system, and then implementing them on the infinite-dimensional system.

Implementation of FDI filters on the infinite-dimensional system

The set of FDI filters and residuals in Eq. 17 were designed to detect and isolate faults in the approximate, finite-dimensional system of Eq. 11. When considering FDI in the infinite-dimensional system of Eqs. 9–10, however, the filters and residuals need to be redesigned on the basis of the actual, not approximate, slow subsystem, since it is x_s, not $\bar{x}_s$, that would be available for measurement under full state feedback conditions. To see how the FDI filters should be modified, consider the following transformation

$$v_s \;=\; \mathcal{T}_s^k x_s \tag{24}$$

which transforms the slow subsystem of Eq. 9 into the following form

$$\begin{aligned}\frac{dv_s}{dt} &= \mathcal{A}_s \mathcal{T}_s^{k^{-1}} v_s + \mathcal{T}_s^k \mathcal{B}_s^k (u^k + f_a^k) + f_s(\mathcal{T}_s^{k^{-1}} v_s, x_f)\\ &:= \tilde{f}_s(v_s, x_f) + \mathcal{D}_s^k (u^k + f_a^k)\end{aligned} \tag{25}$$

where $\tilde{f}_s(v_s, x_f) = \mathcal{A}_s {\mathcal{T}_s}^{k^{-1}} v_s + f_s({\mathcal{T}_s}^{k^{-1}}\ v_s, x_f)$ and $\bar{f}_s(v_s) = \tilde{f}_s(v_s, 0)$. Using the orthogonal projection operators introduced after Eq. 14, $\mathcal{P}_{s_i}$, $i = 1, \ldots, m$, the above system can be written as

$$\frac{dv_{s_i}}{dt} \;=\; \tilde{f}_{s_i}(v_s, x_f) + \mathcal{P}_{s_i} \mathcal{T}_s^k \mathcal{P}_s b_i^k(z)[u_i^k + f_{a_i}^k], \quad i = 1, \ldots, m \tag{26}$$

where $v_{s_i} = \mathcal{P}_{s_i} v_s$, $\tilde{f}_{s_i} = \mathcal{P}_{s_i} \tilde{f}_s$. The FDI filters and residuals can now be redesigned as follows

$$\begin{aligned}&\frac{dw_i}{dt} = \bar{f}_{s_i}(w_i, [v_s]^i) + \mathcal{P}_{s_i} \mathcal{T}_s^k \mathcal{P}_s b_i^k(z) p_i(w_i, [v_s]^i, u^k_{i,\max} \xi^k),\\ &r_i(t) = \|w_i(t) - v_{s_i}(t)\|\end{aligned} \tag{27}$$

for $i = 1, \ldots, m$, where, in lieu of the approximate transformed slow states $\bar{v}_{s_i}$, the exact transformed slow states $\bar{v}_{s_i}$, are used. When comparing the systems of Eq. 26 and Eq. 27, one can observe that each filter essentially simulates the evolution of the i-th slow mode in the absence of faults in the i-th actuator (that is, with $f_{a_i}^k = 0$), and in the absence of the fast states (that is, with $x_f = 0$). The residuals, are, therefore, sensitive not only to faults, but also to approximation errors resulting from neglecting x_f in the design of the filters. This implies that the residuals will be nonzero even in the absence of faults. Note also that, unlike the transformed slow subsystem where the evolution of each state is directly influenced by one input only, each state in the x_f-subsystem is influenced by all inputs. As a result, a fault in some actuator $j \neq i$ will indirectly influence the evolution of the i-th slow mode v_{s_i} (through its effect on x_f), and this will render the residual r_i possibly sensitive to faults in actuators other than the i-th actuator. In other words, the coupling between the slow and fast subsystems destroys the dedicated fault isolation property of the FDI filters designed on the basis of the reduced-order system.

To discriminate between faults and approximation errors (that is, to prevent false alarms), and to ensure that each residual remains practically dedicated to faults in a single actuator, it is important to establish, for each residual, a bound that captures its size in the absence of faults in the corresponding actuator. To allow the derivation of such bounds, we will need to make the following assumption (see Remarks 14–15 for a discussion on how this assumption can be relaxed).

Assumption 4: *Referring to the system of Eqs. 11–12 with* $\bar{x}_s(0) \in \bar{\Omega}_s^k(u_{\max}^k, \xi^k)$, *for a fixed* $k \in \mathcal{K}$, and $f_{a_i}^k \equiv 0$, *for a fixed* $i \in \mathcal{I}$, *there exist positive real numbers,* $\delta_{b_i}^k$ *and* $T_{r_i}^k$, *such that* $\|\bar{x}_s(t)\| \leq \delta_{b_i}^k$ *for all* $t \in [0, T_{r_i}^k]$.

Assumption 4 requires that the states of the closed-loop reduced system be bounded over a finite time-interval in the presence of faults in one or more actuator so long as at least one actuator is healthy. Note that this assumption does not require the origin to be exponentially or asymptotically stable in the presence of faults; only that the system under faults exhibit no finite-escape time, which is reasonable for physical systems. The boundedness assumption allows us to apply singular perturbation techniques to derive a threshold that can be used to uniquely detect and isolate faults in a given actuator. These bounds, which are established in Proposition 3, will be used by the supervisor as FDI thresholds to decide when a fault has occurred in a given actuator and, consequently, when to switch actuator configurations. The proof of this proposition can be found in the Appendix.

Proposition 3: *Consider the closed-loop system of Eqs. 9–10 and Eq. 12, for which Assumption 4 is satisfied, with* $f_{a_i}^k \equiv 0$, *for a fixed* $i \in \mathcal{I}$. *Consider also the transformed slow subsystem of Eq. 26 and the filters of Eq. 27. Then, given the set of positive real numbers* $\{\delta_s^k, \delta_f^k, \delta_{d_i}^k\}$, *where* δ_s^k *as defined in Proposition 1 and* δ_f^k, $\delta_{d_i}^k$, *are arbitrary, there exists a positive real number,* ε', *such that if* $\varepsilon \in (0, \varepsilon']$, $\|x_s(0)\| \leq \delta_s^k$, $\|x_f(0)\|_2 \leq \delta_f^k$, *and* $w_i(0) = v_{s_i}(0)$, *the residual of Eq. 27 satisfies a relation of the form* $r_i(t) \leq \delta_{d_i}^k$ *for all* $t \in [0, T_{r_i}^k]$.

Remark 12: Proposition 3 ties the FDI thresholds, $\delta_{d_i}^k$, to the extent of separation between the slow and fast eigenvalues of the differential operator. Specifically, the thresholds can be chosen by the designer to be arbitrarily small provided that ε is sufficiently small (that is, the FDI filter is of sufficiently high-order). As shown in the Appendix (see Proof of Proposition 3), this connection can be made owing to the boundedness property of the closed-loop system, which allows controlling the closeness between the solution of the reduced system of Eq. 11, and the solution of the slow subsystem of Eq. 9 on a finite time-interval by proper choice of ε. Since the choice of ε fixes the order of the approximate system of Eq. 11, the result of Proposition 3 implies that a tighter FDI threshold (which could be desirable to minimize detection delays) requires a higher-order approximate model. In the asymptotic limit, as the thresholds tend to zero, $\varepsilon \rightarrow 0$ and the FDI filters become infinite-dimensional. Therefore, from a practical implementation standpoint, it is important that the designer carefully balance the resulting tradeoff between the need for tight fault detection criteria and the need to design practically implementable (low-dimensional) filters that are suitable for FDI.

Remark 13: An important aspect that differentiates the result of Proposition 3 from the one derived in[43] for fault detection is the fact that the thresholds introduced here are defined only on a finite time-interval, while the threshold in[43] is defined over the infinite time-interval. One implication of this is that, unlike the fault detection task which can be performed over the infinite time-interval, fault isolation filters designed on the basis of the reduced-order model are capable of isolating faults in the infinite-dimensional system over a finite-time window, whose size is determined by the boundedness of the reduced system. Clearly, the longer the time-interval over which the boundedness assumption is satisfied, the longer the time-window available for fault isolation will be. To understand the difference between the two results, note that in the case of fault detection, the only conclusion of interest is whether some fault has occurred or not. Therefore, to derive a threshold for fault detection purposes, one needs only compare the reduced and infinite-dimensional systems in the absence of all faults to capture the approximation errors that might otherwise be mistaken for faults. Since the reduced system under these conditions is exponentially stable (all actuators are healthy), singular perturbation theory ensures closeness of solutions between the approximate and infinite-dimensional systems over the infinite time-interval, hence, the residual threshold is defined over an infinite time-interval. By contrast, in the case of fault isolation, one seeks to derive, for each residual, a threshold that uniquely identifies faults in a specific actuator. To derive such a threshold, one needs to compare the reduced and infinite-dimensional systems in the absence of faults in this specific actuator (not in all actuators) to capture the expected difference in behavior. Owing to the possible presence of faults in the other actuators, the two systems under comparison are not necessarily exponentially or asymptotically stable, and, therefore, closeness of solutions between the two systems (which determines the size of the residual threshold) is not guaranteed over the infinite time-interval. Instead, singular perturbation results in this case (for example, analogs of Tikhonov's Theorem) guarantee closeness of solutions over a finite time-interval provided that the solution of the reduced system is bounded; hence, the need for Assumption 4.

Remark 14: Note that if Assumption 4 were to be modified to require that the origin of the closed-loop reduced system be exponentially stable in the presence of faults, then it would be possible to derive FDI thresholds over the infinite time-interval. However, such an assumption would be too restrictive in the sense that it limits the types of faults that can be isolated to those that only degrade performance, but do not cause instability. Furthermore, Assumption 4 is not needed if only fault detection is being considered.

Remark 15: The need for residual thresholds stems from the fact that the FDI filters of Eq. 27 use only measurements of the slow states and neglect the fast states. One way to eliminate the need for such thresholds (and the need for Assumption 4 as well) is to include measurements of x_f in the filter design. In this case, the i-th filter equation will be identical to the evolution equation of the i-th transformed slow mode, except for the possible presence of faults in the i-th actuator. In other words, r_i will be nonzero if and only if the i-th actuator is faulty. This can be viewed as a direct generalization of the FDI scheme introduced in the previous section. An important drawback of this approach, however, is that it requires measurements of x_f which are difficult to realize in practice.

Remark 16: It is important to highlight some of the fundamental differences that arise when the above FDI scheme is applied to the linear case. To this end, consider the transformed slow system of Eq. 25 with $f_s(\cdot, \cdot) = 0$. The absence of the nonlinear term, together with the fact that the control action depends on x_s only, implies that the evolution of v_s becomes completely decoupled from x_f. Consequently, the evolution of the i-th filter state becomes identical to that of the i-th transformed slow state with $f_{a_i}^k = 0$, that is unlike the nonlinear case, any discrepancy between v_{s_i} and w_i will be solely due to faults in the i-th actuator, and will not include any approximation errors or any effects of faults in the other actuators. In other words, each residual remains sensitive only to faults in one input, and the dedicated property of the FDI scheme remains exactly preserved when the filter is implemented on the infinite-dimensional linear system. Also, the possibility of false alarms due to model reduction errors in the filter design is precluded in the linear case, and a nonzero FDI threshold similar to the one in Proposition 3 is not needed on account of this fact alone (such a threshold might still be needed when errors due to model uncertainty need to be accounted for).

Implementation of actuator reconfiguration logic on the infinite dimensional system

As discussed earlier, once the faults in the operating control configuration have been detected and isolated, the supervisor needs to select and activate the appropriate fallback actuators (in place of the faulty ones) that preserve closed-loop stability and minimize the deterioration in the closed-loop performance resulting from actuator failure and subsequent switching. For the approximate closed-loop system, the stability component of the actuator switching logic of Eq. 19 is based on monitoring the relative position of the state of the reduced system $\bar{x}_s$, with respect to the stability regions $\bar{\Omega}_s^k$. The same logic applies when considering the infinite-dimensional system except that the supervisor has to monitor the actual slow state x_s with respect to the stability regions Ω_s^k which can be made sufficiently close to $\bar{\Omega}_s^k$ for sufficiently large separation between the slow and fast eigenmodes.

To address the performance objective for the infinite-dimensional system, one may consider the following measure of performance deterioration

$$J(\xi^k) = \int_{T_{d_i}}^{\infty} \left[(e_s(t,\xi^k), \mathcal{Q}_s e_s(t,\xi^k)) + (e_f(t,\xi^k), \mathcal{Q}_f e_f(t,\xi^k)) + e_u^T(x_s(t),\xi^k) R e_u(x_s(t),\xi^k)\right] dt \qquad (28)$$

where T_{d_i} is the time of fault detection, $e_s\,(t,\ \xi^k) := x_s(t;\ x(T_{d_i}),\ \xi^{k(T_{d_i})}) - x_s\,(t;\ x(T_{d_i}),\ \xi^{k(T_{\bar{d}_i})})$, is the discrepancy between the responses of the closed-loop slow subsystems under the original and fallback actuators, $\xi^{k(T_{d_i})}$ is the vector of actuator locations for the fallback configuration to be activated after fault detection, $\xi^{k(T_{\bar{d}_i})}$ is the vector of actuator locations for the faulty configuration to be deactivated, $\mathcal{Q}_s$ is a coercive operator, $e_f(t,\ \xi^k) := x_f(t;\ x(T_{d_i}),\ \xi^{k(T_{d_i})}) - x_f(t;\ x(T_{d_i}),\ \xi^{k(T_{d_i})})$, is the discrepancy between the responses of the closed-loop fast subsystems under the original and fallback actuators, $\mathcal{Q}$ is an unbounded coercive operator, $e_u(x_s(t),\ \xi^k) := p(x_s(t),\ u_{\max}^k,\ \xi^{k(T_{d_i})}) - p(x_s(t),\ u_{\max}^k,\ \xi^{k(T_{\bar{d}_i})})$ is the discrepancy between the two control actions, and R is a positive definite matrix. Note, however, that the evaluation of the cost of Eq. 28 for a given fallback configuration requires simulating the infinite-dimensional closed-loop system (or a sufficiently high-order disrectization thereof), which is not suitable for real-time implementation purposes. To circumvent this problem, we will use the performance functional of Eq. 18 (whose evaluation is computationally feasible) instead as an approximate measure of the performance deterioration associated with each feasible fallback configuration. This choice is justified by the fact that, for sufficiently large separation between the slow and fast eigenmodes, the performance of the finite-dimensional approximate closed-loop system (under a given actuator configuration) can be made arbitrarily close to the performance of the infinite-dimensional system.

We are now ready to proceed with the actuator reconfiguration strategy for the infinite-dimensional system. Theorem 2 that follows establishes that the stability and performance-based actuator reconfiguration logic, based on the finite-dimensional system continues to enforce fault-tolerance in the infinite-dimensional closed-loop system provided that the separation between the slow and fast eigenmodes is large enough. The proof is given in the Appendix.

Theorem 2: *Consider the closed-loop system of Eqs. 9–10 and Eq. 12 with* $k(0) = j \in \mathcal{K}$, *and the system of Eq. 27 with* $w_i(0) = v_{s_i}\,(0)$. *Then, given the set of positive real numbers,* $\{\delta_s^j,\ \delta_f^j,\ \delta_{d_i}^j\}$, *where* δ_s^j *was defined in Proposition 1 and* δ_f^j, $\delta_{d_i}^{\ j}$ *are arbitrary, and given any fault,* $f_{a_i}^{\ j}$, *for which* $r_i(T_{d_i}) > \delta_{d_i}^j$, *where* $T_{d_i} := \min\ \{t \in [0,\ T_{r_i}^j]:\ r_i(t) > \delta_{d_i}^j\}$, *for some* $i = 1, \ldots, m$, *there exists* $\varepsilon^s > 0$ *such that if* $\varepsilon \in (0,\ \varepsilon^s]$, $\|x_s(0)\| \leq \delta_s^j$, $\|x_f(0)\|_2 \leq \delta_f^j$, $w_i(0) = v_{s_i}(0)$, *the control-reconfiguration rule given by*

$$k(t) \;=\; \left\{\begin{array}{ll} j, & 0 \leq t < T_{d_i} \\ \mu, & t \geq T_{d_i} \end{array}\right\} \qquad (29)$$

where $\xi^{\mu} = \arg\min_{v\in D} \bar{J}(\xi^{v})$ *and* $\mathcal{D} := \{v \neq j : x_s(T_{d_i}) \in \Omega_s^v,\ \xi_a^{\,v} = \xi_a^j,\ a \neq i\}$, *ensures that:*

1. *the origin of the closed-loop system is asymptotically stable, and*
2. *the actuator configuration* $k = \mu$ *is near-optimal in the sense that* $J(\xi^{\mu}) \rightarrow \bar{J}_s(\xi^{\mu})$ *as* $\varepsilon \rightarrow 0$.

Remark 17: Theorem 2 considers faults that are observable from the filters' residuals in the sense that a residual in excess of the allowable threshold $\delta_{d_i}^k$ is a conclusive indicator that a fault has occurred in the i-th actuator, since $r_i > \delta_{d_i}^k$ is more than what can be accounted for by inherent approximation errors. Faults that yield a residual within the margin of (that is, indistinguishable from) these errors are not considered since their effect on closed-loop stability cannot be discerned from the behavior of the residual. Note, however, that the observability threshold, $\delta_{d_i}^k$, can be chosen arbitrarily small by appropriate selection of ε, thus, rendering the possibility of major (that is, destabilizing) faults that cannot be detected quite small. Note also that reducing the threshold requires increasing the dimension of

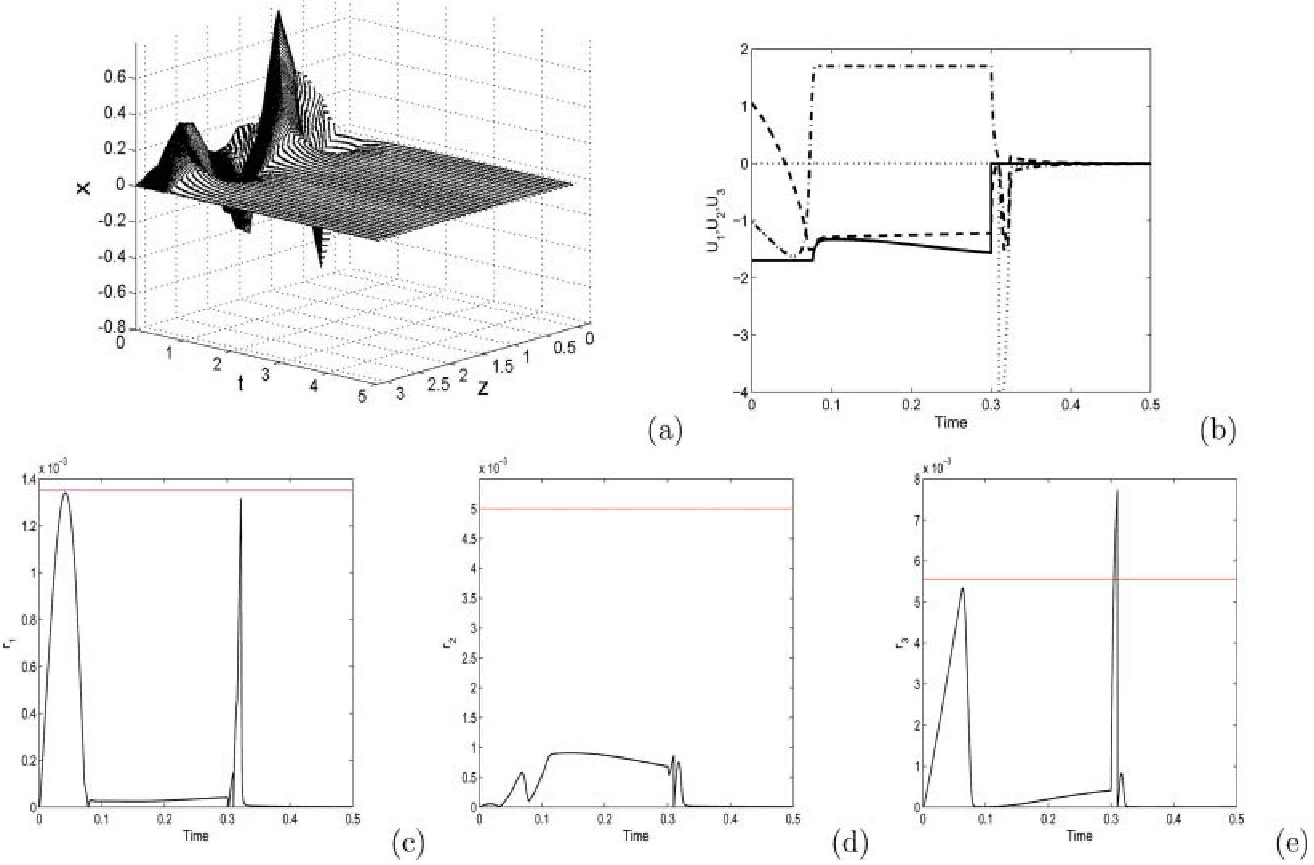

Figure 2. Evolution of: (a) the closed-loop temperature profile, (b) the manipulated input profiles, and (c)–(e) the FDI filter residuals, when failure is detected in actuator *C* at *t* = 0.305, and actuator *D* is activated immediately.

The solid and dotted lines in (b) describe the manipulated input profiles for actuators *C* and *D*, respectively. [Color figure can be viewed in the online issue, which is available at www.interscience.wiley.com.]

the slow subsystem to reduce the approximation errors. Ultimately, the choice of $\delta_{d_i}^k$ reflects a fundamental tradeoff between the need to avoid false alarms that could be caused by approximation errors (this favors a relatively large threshold), and the need to minimize the possibility of some faults going undetected (this favors a relatively small threshold).

Remark 18: The results of Theorems 1 and 2 can be generalized, in a conceptually straightforward fashion, to handle the case of multiple consecutive faults. Note that once the fallback actuator configuration is switched-in following the detection of faults in the operating control configuration, the structure of the input operator changes due to the change in actuator locations. To maintain the ability to detect and isolate future faults in the newly activated configuration, it is important that the locations of the fallback actuators be chosen, such that the new input operator is invertible. This allows transforming the new slow subsystem into a diagonal form similar to that of Eq. 26, and building a new set of dedicated FDI filters.

Remark 19: In the presence of plant-model mismatch or unknown disturbances, the residual will be nonzero, and can exceed the alarm threshold even in the absence of faults. False detection alarms can trigger unnecessary, or premature, control system reconfiguration that destabilizes the closed-loop system or significantly degrades its performance. The FDI-FTC problem in the presence of time-varying uncertainties with known bounds on the uncertainties can be handled by: (1) redesigning the FDI filters to account for the uncertainty—either by modifying the FDI criteria to require that a fault be declared only if the value of the residual increases beyond some threshold that accounts for the deviation of the plant dynamics from the nominal dynamics in the absence of faults, or by redesigning the filter using the unknown input observer principle (for example,[2,12,52]) to decouple the effect of uncertainty on the residual, (2) redesigning the controllers for the individual control configurations to attenuate the effect of uncertainty on the process, and (3) characterizing the regions of robust stability for the various controllers, and using them as the basis for deriving a set of robust switching laws that orchestrate safe transitions from the faulty to the healthy actuators in a way that ensures robust stability in the overall switched closed-loop system. Some preliminary results on robust fault detection and handling in uncertain transport-reaction processes are reported in.[53]

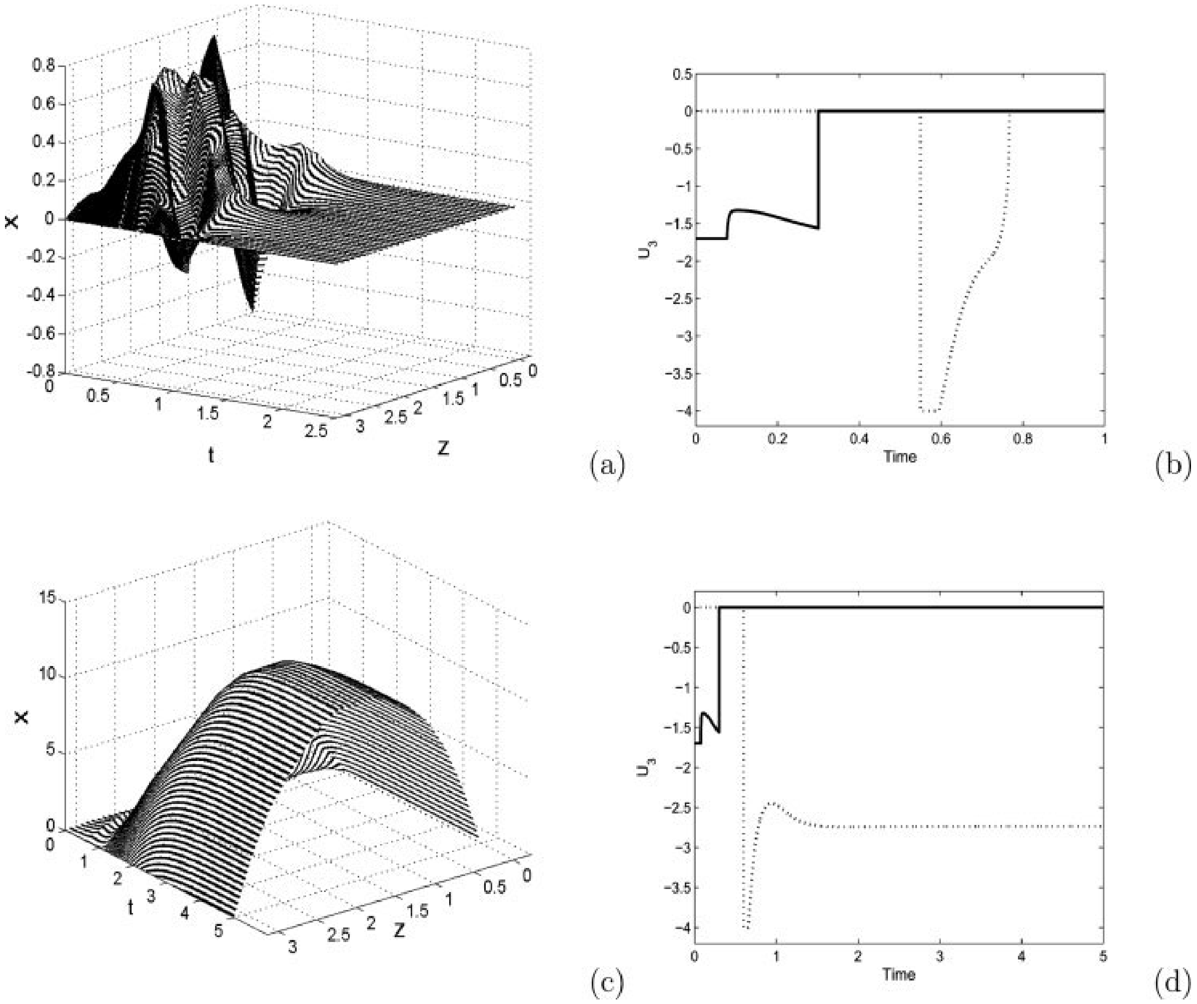

Figure 3. Evolution of the closed-loop temperature and manipulated input profiles when failure is detected in actuator *C* at *t* = 0.305, and actuator *D* is activated at *t* = 0.5 (plots (a) and (b)), and when actuator *D* is activated at *t* = 0.6 (plots (c) and (d)).

The solid and dotted lines in (b) and (d) describe the manipulated input profiles for actuators *C* and *D*, respectively.

Remark 20: In the fault-tolerant control methodology presented in this work, it is assumed that the number of control actuators used at any given time is that necessary for enforcing the desired closed-loop stability and performance properties under constraints. As a result, the failure of one or more control actuators will lead (in the absence of any corrective action) to closed-loop instability and/or unacceptable performance deterioration, and, thus, necessitates switching to healthy and feasible fallback actuators in order to preserve closed-loop stability and minimize performance degradation (that is, active fault-tolerant control). The use of as many control actuators as is necessary at a time is typically motivated by economic considerations (for example, the need to save on unnecessary control effort). However, it is possible (as is done in reliable control approaches[22]) to use more control actuators than is necessary (possibly all the available actuators) at any given time so as to reduce the possibility of total failure in the control structure following the failure of some of the actuators. In this case, fault-tolerance can be achieved without active switching or actuator reconfiguration (that is, passive fault-tolerant control), provided that the remaining actuators have sufficient control authority to prevent instability and/or significant performance losses. Unless the control actuator locations are chosen to ensure controllability under the remaining actuators, and the control laws used by the remaining actuators are redesigned (based on the new structure of the input operator), there can be no guarantee that the remaining actuators will be sufficient to enforce fault-tolerance. In this case, a graceful shut down of the process may become unavoidable.

Application to a Diffusion-Reaction Process

In this section, we demonstrate and evaluate, through computer simulations, the implementation of the third-order model-based FDI-FTC scheme designed in Eqs. 21–23 on the diffusion-reaction process of Eqs. 7–8. In all simulation

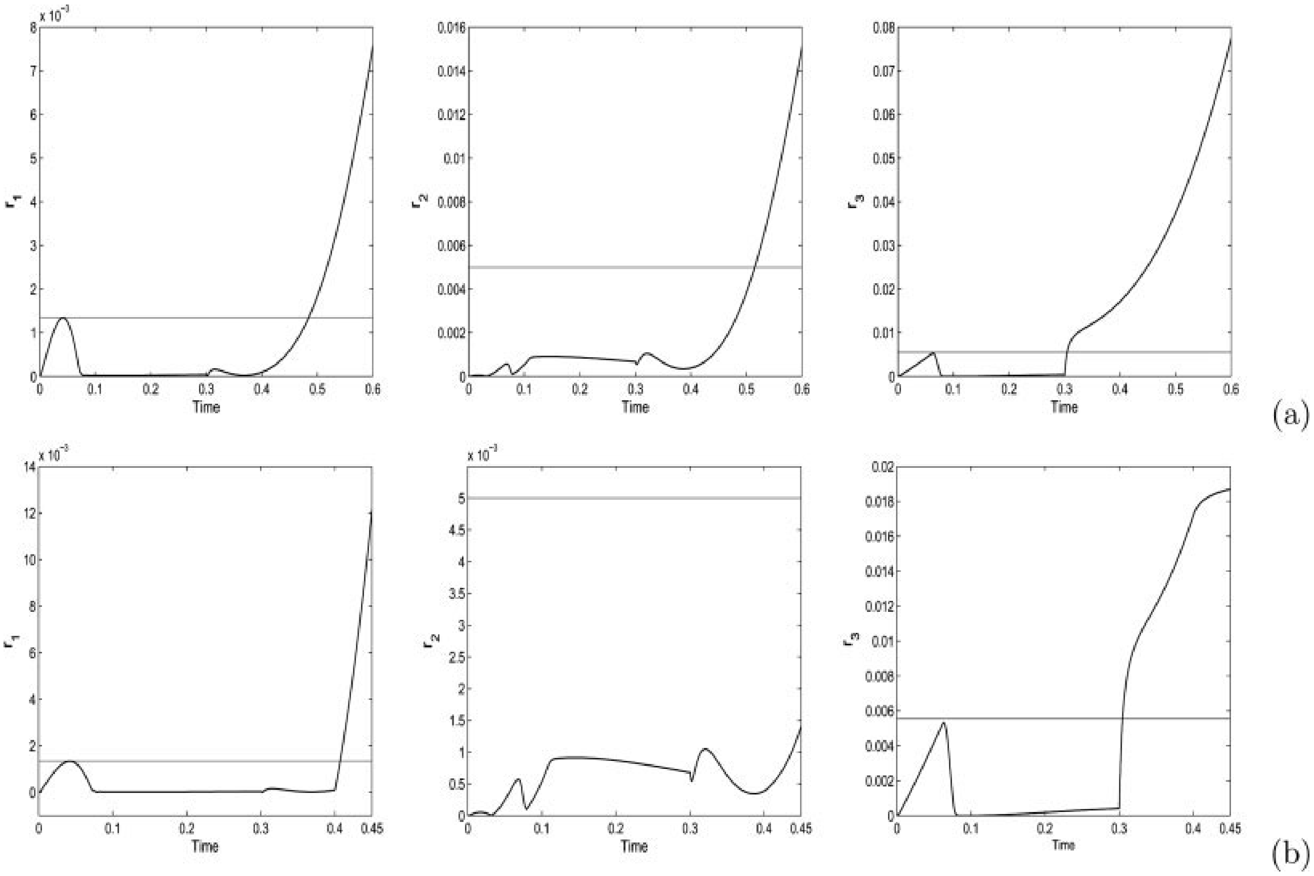

Figure 4. Evolution of the FDI filter residuals (with low-thresholds) when actuator *C* fails at $t = 0.3$, and: (a) no additional faults occur afterwards, and (b) a second fault in actuator *A* occurs at $t = 0.4$.

runs, the controller of Eqs. 20–21 and the FDI filters of Eq. 23 are implemented on a 30-th order Galerkin's discretization of the parabolic PDE (higher-order discretizations led to identical results), starting from the initial profile $\bar{x}(z, 0) := x_0(z) = \Sigma_{i=1}^{3} a_i(0)\phi_i(z)$, with $a_1(0) = 0.18$, $a_2(0) = a_3(0) = 0.2$. It was verified that the controller successfully stabilizes the temperature at the desired, spatially-uniform steady-state using actuator configuration (*A*, *B*, *C*) in the absence of faults.

We now turn to the case when the control system operation is interrupted by actuator faults. Since the residuals are expected to be nonzero (even in the absence of faults), due to the model reduction errors in the filters design, we use the following criteria $r_i(t) \geq \delta_i$, to declare a fault in a given actuator at a given time. For the given initial condition, it was found that $\delta_1 = 0.0014$, $\delta_2 = 0.0050$ and $\delta_3 = 0.0056$ were suitable choices. We consider first the case of faults in a single actuator. To this end, the dimensionless rod temperature is initialized at $x_0(z)$, using actuator configuration (*A, B, C*), and the filters of Eq. 23 are initialized at $w_i(0) = v_i(0)$, for $i = 1, 2, 3$. At $t = T_{f_1} = 0.3$, failure is introduced in actuator *C* (see the solid line in Figure 2b). As shown in the residual profiles in Figure 2c–2e this failure is detected and isolated almost immediately by the supervisor since it causes r_3 to cross the threshold at $T_{d_1} = 0.305$. Note that neither of the other two residuals exceeds its specified threshold at this time, indicating that no faults can be declared in actuators *A* and *B*. Note also that following the detection, all residuals are re-initialized by the supervisor. To determine which backup actuator (*D*, *E*, or *F*) is suitable for use in place of actuator *C*, we follow the same switching logic based on the reduced-order model and activate actuator *D* owing to its desirable stability and performance properties. The resulting closed-loop temperature and manipulated input profiles are shown in Figure 2a–2b for the case when actuator re-configuration happens immediately following FDI with no delays. Figure 3 shows the results when actuator *D* is activated at $t = 0.5$ (plots (a) and (b)) and at $t = 0.6$ (plots (c) and (d)). Delays between FDI and reconfiguration can arise, for example, due to the time needed to carry out the computations necessary to determine the optimal backup actuator. As expected, closed-loop stability can be maintained in the presence of a small delay but may be lost under larger delays.

It should be noted that in the case of delays between FDI and actuator reconfiguration, the residuals cannot be reset to zero until the new backup actuator is activated. Therefore, it is important to continue to monitor the evolution of the residuals after FDI of the first fault to determine whether additional faults have occurred in the other actuators during the delay period. Caution must be exercised, however, when interpreting the residual evolution during this period in order

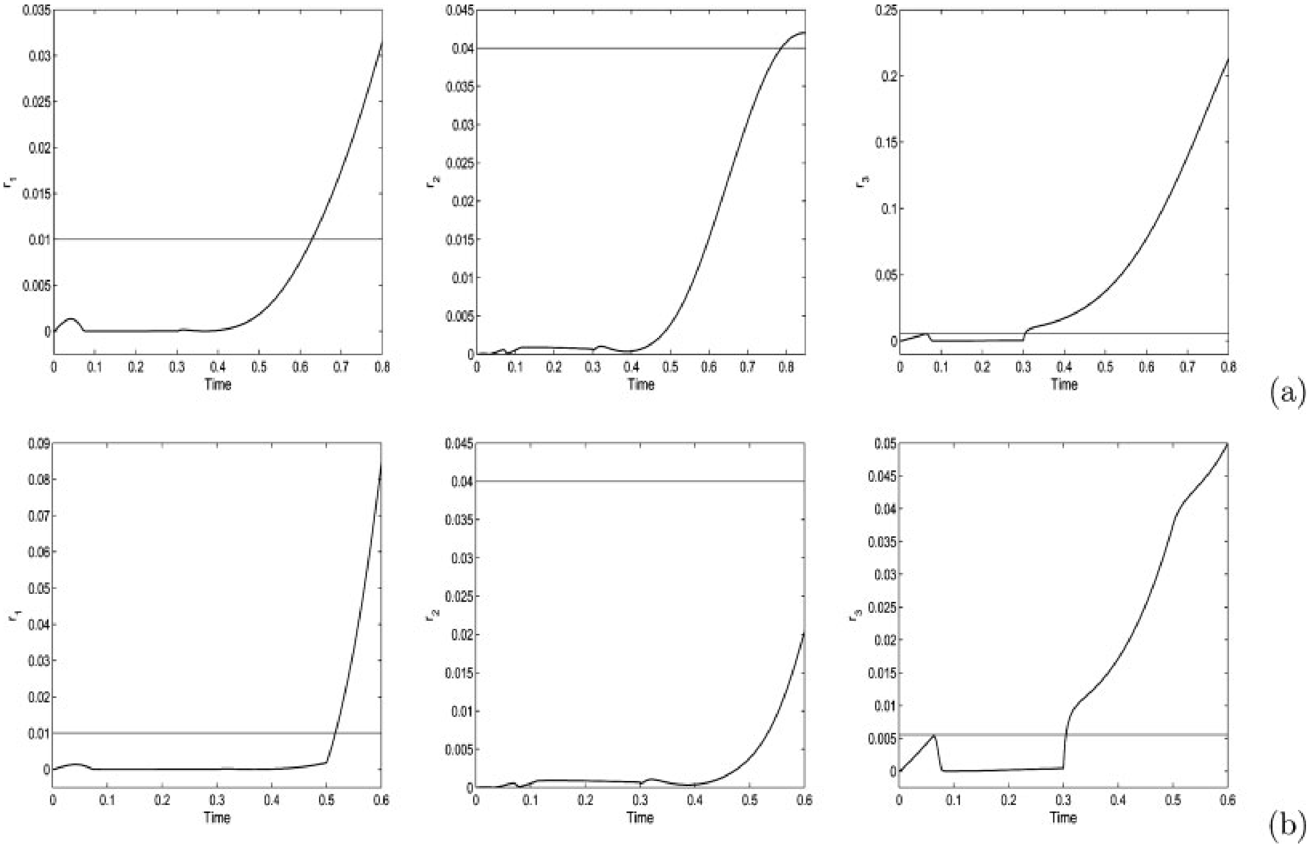

Figure 5. Evolution of the FDI filter residuals (with high-thresholds), when actuator *C* fails at *t* = 0.3 and: (a) no additional faults occur afterwards, and (b) a second fault in actuator *A* occurs at *t* = 0.5.

to avoid false alarms. During the delay period, the process is evolving under a faulty actuator configuration and, if the delay is sufficiently long, this can cause the residuals of the healthy actuators to cross their specified thresholds (note that the thresholds capture the residual sizes in the absence of faults in any of the actuator) thus leading to false alarms. To illustrate this point, we consider the case when actuator C fails at $t = 0.3$ but re-configuration to actuator D is delayed until $t = 0.55$. Figure 4a shows the evolution of the three residuals during the delay period. We observe that, while r_3 crosses its threshold as expected shortly after the occurrence of the failure, both r_1 and r_2 also cross their thresholds at $t = 0.485$ and $t = 0.515$, respectively, even though no faults were introduced into either actuator A or B. Misinterpreting these crossings as faults can lead to unnecessary actuator re-configuration and possibly closed-loop instability. One way to avoid these false alarms is to limit the FDI time window to a finite time-interval whose size is dictated by the duration between the detection of the first fault ($t = 0.305$), and the first crossing ($t = 0.485$). Having r_1 or r_2 cross its threshold during this time period is conclusive indicator that a fault in actuator A or B, respectively, has occurred. This is shown in Figure 4b, where a second fault in actuator A occurs within the allowable time window at $t = 0.4$, and is detected by r_1 crossing its threshold at $t = 0.407$. This finding is consistent with the result of Proposition 3 regarding FDI on a finite time-interval when the reduced-order model-based filters are implemented on the infinite-dimensional system.

It should be noted that the FDI time window can be increased if the thresholds are appropriately increased. For example, Figure 5a shows that with a choice of $\delta_1 = 0.01$ and $\delta_2 = 0.04$, and in the absence of faults in actuators A and B, r_1 and r_2 cross their thresholds at $t = 0.629$ and $t = 0.788$, respectively (compare with Figure 4a, where the crossings occurred earlier). The new FDI time window now spans the interval from $t = 0.305$ to $t = 0.629$, and, thus, covers the entire delay period, which allows the detection and isolation of faults in A or B during that time. Figure 5b shows the case when a fault in actuator A is introduced at $t = 0.5$, and detected by r_1 crossing its threshold within the allowable time window (detection occurs at $t = 0.516$). Note that, using the previous low thresholds and smaller time window, it would not have been possible to detect this fault.

Finally, to demonstrate the importance of monitoring the residuals during the delay period, we consider the case when, following the detection of failure in actuator C at $t = 0.305$, a fault occurs in actuator A at $t = 0.5$ (that is, during the delay period), and compare the behavior of the closed-loop system when such fault is ignored and when it is accounted for. By disregarding the evolution of the residuals during the delay period, the failure in actuator A will go undetected, and the supervisor will activate actuator D in place of actua-

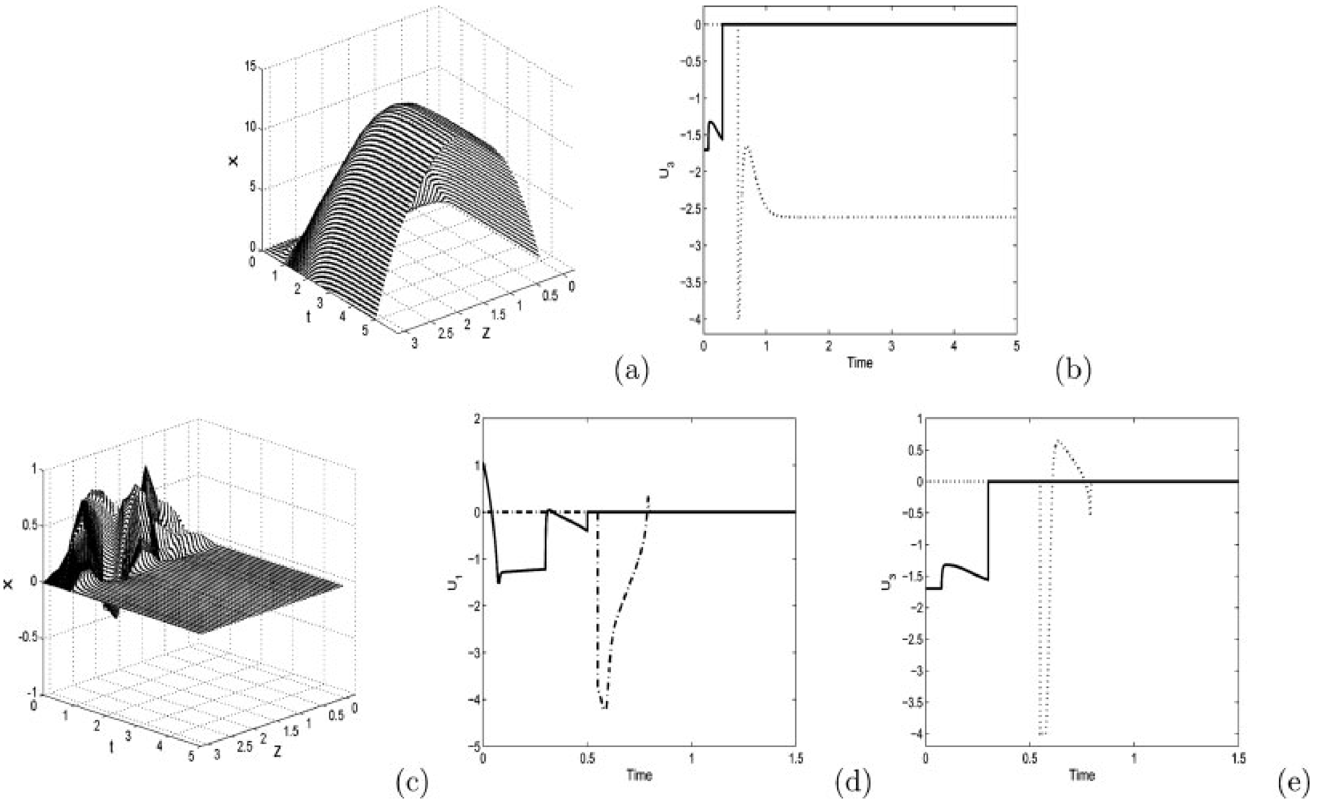

Figure 6. Evolution of the closed-loop temperature and manipulated input profiles, when consecutive failures in actuators *C* and *A* occur at *t* = 0.3, and *t* = 0.5, respectively.

In plots (a)–(b) failure in actuator *A* goes undetected and only actuator *C* is replaced by *D* at $t = 0.55$. The solid and dotted lines in (b) describe the manipulated input profiles for actuators *C* and *D*, respectively. In plots (c)–(e) both actuators, *C* and *A*, are replaced by *D* and *E*, respectively at $t = 0.55$. The solid and dotted lines in (d) describe the manipulated input profiles for actuators *A* and *E*, respectively, while the solid and dotted lines in (e) describe the manipulated input profiles for actuators *C* and *D*, respectively.

tor *C* (following the same switching logic considered in Figure 2) at the end of the delay period at $t = 0.55$. The result is shown in Figure 6a–6b which demonstrates that the closed-loop system becomes unstable. By contrast, when the failure in actuator *A* is detected and isolated by monitoring the evolution of the residuals in Figure 5b, and the supervisor replaces actuators *C* and *A* with healthy actuators *D* and *E*, respectively, at $t = 0.55$, closed-stability is maintained as shown in Figure 6c–6e.

Conclusions

A model-based FTC structure integrating feedback control, FDI and performance-based reconfiguration was developed for transport-reaction processes modeled by nonlinear parabolic PDEs with control constraints and actuator faults. Initially, model reduction techniques were used to obtain a finite-dimensional system that approximates the dominant dynamic modes of the PDE. The approximate model was then used to synthesize, for each actuator configuration, a stabilizing nonlinear feedback controller and characterize its stability region in terms of the control constraints and actuator locations. A set of dedicated FDI filters, each replicating the fault-free behavior of a given dominant mode, was then constructed, and the discrepancy between the evolution of the fault-free and actual modes were used as residuals. The actuator locations were chosen to ensure that the residual of each filter is sensitive to faults in only one actuator. Following FDI, a set of actuator reconfiguration rules were derived to preserve closed-loop stability and minimize the closed-loop performance deterioration resulting from faults. Appropriate FDI thresholds and control reconfiguration criteria that take the inherent approximation errors into account when implementing the fault-tolerant control structure on the process were derived to guard against false alarms. Finally, the integrated control, FDI and reconfiguration methodology was applied to the problem of actuator fault-tolerant stabilization of an unstable steady-state of a diffusion-reaction process.

Literature Cited

1. Himmelblau DM. *Fault Detection and Diagnosis in Chemical and Petrochemical Processes*. New York: Elsevier Scientific Pub.; 1978.
2. Simani S, Fantuzzi C, Patton R. *Model-based Fault Diagnosis in Dynamic Systems Using Identification Techniques*. London: Springer; 2003.
3. Blanke M, Kinnaert M, Lunze J, Staroswiecki M. *Diagnosis and Fault-Tolerant Control*. Berlin-Heidelberg: Springer; 2003.
4. Kresta JV, Macgregor JF, Marlin TE. Multivariate statistical monitoring of process operating performance. *Can J Chem Eng*. 1991; 69:35–47.
5. Rollins DR, Davis JF. Unbiased estimation of gross errors when the covariance matrix is unknown. *AIChE J*. 1993;39:1335–1341.

6. Negiz A, Cinar A. Statistical monitoring of multivariable dynamic processes with state-space models. *AIChE J*. 1997;43:2002–2020.
7. Davis JF, Piovoso ML, Kosanovich K, Bakshi B. Process data analysis and interpretation. *Adv Chem Eng*. 1999;25:1–103.
8. Tatara E, Cinar A. An intelligent system for multivariate statistical process monitoring and diagnosis. *ISA Transactions*. 2002;41:255–270.
9. Zhang XD, Parisini T, Polycarpou MM. Adaptive fault-tolerant control of nonlinear uncertain systems: An information-based diagnostic approach. *IEEE Trans Automat Contr*. 2004;49:1259–1274.
10. Mehranbod N, Soroush M, Panjapornpon C. A method of sensor fault detection and identification. *J Proc Contr*. 2005;15:321–339.
11. Massoumnia M, Verghese GC, Wilsky AS. Failure detection and identification. *IEEE Trans Automat Contr*. 1989;34:316–321.
12. Frank PM. Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy - a survey and some new results. *Automatica*. 1990;26:459–474.
13. Frank PM, Ding X. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *J Proc Contr*. 1997;7:403–424.
14. Kazantzis N, Kravaris C, Wright RA. Nonlinear observer design for process monitoring. *Ind & Eng Chem Res*. 2000;39:408–419.
15. Saberi A, Stoorvogel AA, Sannuti P, Niemann H. Fundamental problems in fault detection and identification. *Int J Rob & Non Contr*. 2000;10:1209–1236.
16. DePersis C, Isidori A. A geometric approach to nonlinear fault detection and isolation. *IEEE Trans Automat Contr*. 2001;46:853–865.
17. Huang B. Detection of abrupt changes of total least squares models and application in fault detection. *IEEE Trans Contr Syst Tech*. 2001;9:357–367.
18. Cheng L, Kwok E, Huang B. Closed-loop fault detection using local approach. *Can J Chem Eng*. 2003;81:1101–1108.
19. Kazantzis N, Huynh N, Wright RA. Nonlinear observer design for the slow states of a singularly perturbed system. *Comp & Chem Eng*. 2005;29:797–806.
20. El-Farra NH, Christofides PD. Coordinating feedback and switching for control of hybrid non-linear processes. *AIChE J*. 2003;49:2079–2098.
21. Christofides PD, El-Farra NH. Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-Delays, 446 pages. Berlin, Germany: Springer-Verlag; 2005.
22. Yang GH, Wang JL, Soh YC. Reliable H_∞ control design for linear systems. *Automatica*. 2001;37:717–725.
23. Bao J, Zhang WZ, Lee PL. Decentralized fault-tolerant control system design for unstable processes. *Chem Eng Sci*. 2003;58:5045–5054.
24. Friedman A. *Partial Differential Equations*. New York: Holt, Rinehart & Winston; 1976.
25. Ray WH. *Advanced Process Control*. New York: McGraw-Hill; 1981.
26. Skliar M, Ramirez WF. Source identification in the distributed parameter systems. *Appl Math & Comp Sci*. 1998;8:733–754.
27. Christofides PD, Daoutidis P. Nonlinear control of diffusion-convection-reaction processes. *Comp & Chem Eng*. 1996;20:1071–1076.
28. Christofides PD. *Nonlinear and Robust Control of PDE Systems: Methods and Applications to Transport-Reaction Processes*. Boston: Birkhäuser; 2001.
29. Palazoglu A, Karakas A. Control of nonlinear distributed parameter systems using generalized invariants. *Automatica*. 2000;36:697–707.
30. Alonso A, Ydstie BE. Stabilization of distributed systems using irreversible thermodynamics. *Automatica*. 2001;37:1739–1755.
31. Ruszkowski M, Garcis-Osorio V, Ydstie BE. Passivity based control of transport reaction systems. *AIChE J*. 2005;51:3147–3166.
32. Hoo KA, Zheng DG. Low-order control-relevant models for a class of distributed parameter systems. *Chem Eng Sci*. 2001;50:6683–6710.
33. El-Farra NH, Armaou A, Christofides PD. Analysis and control of parabolic PDE systems with input constraints. *Automatica*. 2003;39:715–725.
34. Dubljevic S, Mhaskar P, El-Farra NH, Christofides PD. Predictive control of transport-reaction processes. *Comp & Chem Eng*. 2005;29:2335–2345.
35. Dochain D. State observation and adaptive linearizing control for distributed parameter (bio)chemical reactors. *Inter J Adapt Contr & Sig Proc*. 2001;15:633–653.
36. Armaou A, Demetriou MA. Optimal actuator/sensor placement for linear parabolic PDEs using spatial H_2 norm. *Chem Eng Sci*. 2006;61:7351–7367.
37. Baruh H. Actuator failure detection in the control of distributed systems. *J of Guidance, Control, and Dynamics*. 1986;9:181–189.
38. Demetriou M, Ackleh AS, Reich S. Detection and accommodation of second order distributed parameter systems with abrupt changes in the input term: Existence and approximation. *Kybernetika*. 2000;36:117–132.
39. Demetriou M. Robust fault tolerant controller in parabolic distributed parameter systems with actuator faults. In: *Proceedings of 42th IEEE Conference on Decision and Control*. Maui, Hawaii, USA; 2003. p. 324–329.
40. Demetriou M, Kazantzis N. A new actuator activation policy for performance enhancement of controlled diffusion processes. *Automatica*. 2004;40:415–421.
41. El-Farra NH, Christofides PD. Coordinated feedback and switching for control of spatially-distributed processes. *Comp & Chem Eng*. 2004;28:111–128.
42. El-Farra NH, Lou Y, Christofides PD. Fault-tolerant control of fluid dynamic systems: Coordinated feedback and switching. *Comp & Chem Eng*. 2003;27:1913–1924.
43. El-Farra NH. Integrated model-based fault detection and fault-tolerant control architectures for distributed processes. *Ind & Eng Chem Res*. 2006;45:8338–8351.
44. Christofides PD, Daoutidis P. Finite-dimensional control of parabolic PDE systems using approximate inertial manifolds. *J Math Anal Appl*. 1997;216:398–420.
45. El-Farra NH, Ghantasala S. Integrating actuator/sensor placement and fault-tolerant output feedback control of distributed processes. In: *Proceedings of American Control Conference, to appear*. New York, NY; 2007.
46. Lin Y, Sontag ED. A universal formula for stabilization with bounded controls. *Sys & Contr Lett*. 1991;16:393–397.
47. El-Farra NH, Mhaskar P, Christofides PD. Hybrid predictive control of nonlinear systems: Method and applications to chemical processes. *Inter J Rob & Non Contr*. 2004;14:199–225.
48. Halim D, Moheimani SR. An optimization approach to optimal placement of collocated piezo-electric actuators and sensors on a thin plate. *Mechatronics*. 2003;13:27–47.
49. Curtain RF, Zwart HJ. *An Introduction to Infinite Dimensional Linear Systems Theory. Texts in Applied Mathematics*, Berlin: Springer; 1995;21.
50. Dubljevic S, Kazantzis N. A new Lyapunov design approach for nonlinear systems based on zubov's method. *Automatica*. 2002;38:1999–2007.
51. El-Farra NH, Mhaskar P, Christofides PD. Hybrid predictive control of nonlinear systems: Method and applications to chemical processes. *Inter J Rob & Non Contr*. 2004;14:199–225.
52. Watanabe K, Himmelblau DM. Instrument fault detection in systems with uncertainties. *Inter J Syst Sci*. 1982;13:137–158.
53. Ghantasala S, El-Farra NH. Robust fault detection and handling in control of uncertain transport-reaction processes, to appear. In: *Proceedings of 8th International Conference on Dynamics and Control of Process Systems*. Cancun, Mexico; 2007.
54. Khalil HK. Nonlinear Systems. 2nd ed. Upper Saddle River, New Jersey: Prentice Hall; 1996.

Appendix

Proof of Proposition 1: In this proof, we show that the i-th filter detects and isolates a fault in the i-th actuator if and only if one occurs. To this end, consider the systems of Eqs. 16–17, and let $\bar{v}_{s_i}(\bar{T}_{\mathrm{d}_i}) := \bar{v}_{s_i}^{d}$ and $\bar{w}_i(\bar{T}_{d_i}) := \bar{w}_i^{d}$. Then, we have

$$\begin{aligned}\dot{\bar{w}}_i(\bar{T}_{d_i}) - \dot{\bar{v}}_{s_i}(\bar{T}_{d_i}) = &\bar{f}_{s_i}(\bar{w}_i^d, [\bar{v}_s^d]^i) - \bar{f}_{s_i}(\bar{v}_{s_i}^d, [\bar{v}_s^d]^i)\\ &+ \mathcal{P}_{s_i}\mathcal{T}_s^j\mathcal{P}_s b_i^j(z)[p_i(\bar{w}_i^d, [\bar{v}_s^d]^i, u_{i,\max}^j, \xi^j) - p_i(\bar{v}_{s_i}^d, [\bar{v}_s^d]^i, u_{i,\max}^j\xi^j)]\\ &- \mathcal{P}_{s_i}\mathcal{T}_s^j\mathcal{P}_s b_i^j(z)f_{a_i}^j(\bar{T}_{d_i})\end{aligned} \tag{30}$$

with $f^j_{a_i}$ $(\overline{T}_{d_i}) \neq 0$. Since $\overline{w}_i(0) = \overline{v}_{s_i}(0)$ and $f^j_{a_i}$ (t) $\equiv$ 0 for all $0 \leq t < \overline{T}_{d_i}$, we have $\overline{w}^d_i = \overline{v}^d_{s_i}$, which implies that $p_i(\overline{w}^d_i$, $[\overline{v}_s{}^d]^i$, $u^j_{i,\max}$, $\xi^j) - p_i(\overline{v}^d_{s_i}$, $[\overline{v}^d_s]^i$, $u^j_{i,\max}$, $\xi^j)$, $= 0$ and $\overline{f}_{s_i}(\overline{w}_i{}^d$, $[\overline{v}_s{}^d]^i) - \overline{f}_{s_i}(\overline{v}_{s_i}{}^d$, $[\overline{v}_s{}^d]^i) = 0$. Substituting these relations into Eq. 30 yields $\bar{w}_i(\overline{T}_{d_i}) - \bar{v}_{s_i}(\overline{T}_{d_i}) = -\mathcal{P}_{s_i}\mathcal{T}^j_s\mathcal{P}_s b^j_i(z) f^j_{a_i}(\overline{T}_{d_i})$. Since $\mathcal{P}_{s_i}\mathcal{T}^j_s\mathcal{P}_s b^j_i(z) \neq 0$, it follows that $\bar{w}_i(\overline{T}_{d_i}) - \bar{v}_{s_i}(\overline{T}_{d_i}) \neq 0$ if and only if $f^j_{a_i}(\overline{T}_{d_i}) \neq 0$. This, together with the fact that $\overline{w}^d_i = \overline{v}^d_{s_i}$, implies that $\overline{w}_i(\overline{T}_{d_i}{}^+) - \overline{v}_{s_i}$ $(\overline{T}^+_{d_i}) \neq 0$, that is $\overline{r}_i(\overline{T}^+_{d_i})$ $:= \|\overline{w}_i(\overline{T}^+_{d_i}) - \overline{v}_{s_i}$ $(\overline{T}^+_{d_i})\| > 0$, if and only if $f^j_{a_i}(\overline{T}_{d_i}) \neq 0$. This completes the proof of the proposition.

Proof of Theorem 1: Note first that in the absence of faults (that is, $f^j_{a_i}(t)$ $\equiv$ 0 for all $t \geq 0$ and $i \in \mathcal{I}$), we have from Proposition 1 that $\overline{r}_i(t) = 0$ for all $t \geq 0$. From the definition of $\overline{T}_{d_i}$ in Theorem 1, we conclude that $\overline{T}_{d_i} = \infty$, which implies that $k(t) = j$ for all $t \geq 0$ from Eq. 19. Since $\overline{x}_s(0) \in \overline{\Omega}^j_s$, and control configuration j is implemented for all times in this case, closed-loop stability follows directly from Assumption 2.

In the case of faults, the earliest time a fault in the i-th actuator is detected is $\overline{T}_{d_i}$, and we have from Eq. 19 that $k(t) = j$ for $0 \leq t < \overline{T}_{d_i}$. From the stability of the j-th closed-loop system (Assumption 2), we have that the closed-loop state trajectory stays bounded, that is $\overline{x}_s(t) \in \Omega_s{}^j(u^j_{\max}$, $\xi^j)$ for $0 \leq t < \overline{T}_{d_i}$. At time $\overline{T}_{d_i}$, the supervisor switches to control configuration $k = \mu$, for which $\overline{x}_s(\overline{T}_{d_i}) \in \overline{\Omega}^\mu_s(u^\mu_{\max}$, $\xi^\mu)$, and implements it in the closed-loop system for all future times, thus, achieving closed-loop stability. This completes the proof of the theorem.

Proof of Proposition 3: Consider the closed-loop system of Eqs. 9–10 and Eq. 12 with $f^k_{a_i} = 0$, for a fixed $i \in \mathcal{I}$, and the i-th filter of Eq. 27. Using the transformation of Eq. 24, and the orthogonal projection operators $\mathcal{P}_{s_i}$, the closed-loop system plus the filter can be written in the following form

$$
\begin{aligned}
\frac{dv_{s_i}}{dt} &= \tilde{f}_{s_i}(v_s, x_f) + \mathcal{P}_{s_i}\mathcal{T}^k_s\mathcal{P}_s b^k_i(z) p_i(v_s, u^k_{i,\max},\ \xi^k) \\
\frac{dw_i}{dt} &= \bar{f}_{s_i}(w_i, [v_s]^i) + \mathcal{P}_{s_i}\mathcal{T}^k_s\mathcal{P}_s b^k_i(z) p_i(w_i, [v_s]^i, u^k_{i,\max},\ \xi^k) \\
\frac{dv_{s_j}}{dt} &= \tilde{f}_{s_j}(v_s, x_f) + \mathcal{P}_{s_j}\mathcal{T}^k_s\mathcal{P}_s b^k_j(z) \\
&\qquad \times [p_j(v_s, u^k_{j,\max},\ \xi^k) + f^k_{a_j}],\ \ j = 1, \ldots, m, \quad j \neq i \\
\frac{dx_f}{dt} &= \mathcal{A}_f x_f + \mathcal{B}^k_f[p(v_s, u^k_{\max},\ \xi^k) + f^k_a] + f_f(x_s, x_f)
\end{aligned}
\tag{31}
$$

Using the fact that $\varepsilon = \frac{|Re\{\lambda_m\}|}{|Re\{\lambda_{m+1}\}|} < 1$ and multiplying the x_f-subsystem by ε, the above system can be put in the standard singularly perturbed form, with v_{s_i}, w_i, and v_{s_j} being the slow states, and x_f being the fast states. Applying standard two time-scale decomposition, it can be verified that the fast subsystem is globally exponentially stable, and that the reduced closed-loop slow system takes the form

$$
\begin{aligned}
\frac{d\bar{v}_{s_i}}{dt} &= \bar{f}_{s_i}(\bar{v}_s) + \mathcal{P}_{s_i}\mathcal{T}^k_s\mathcal{P}_s b^k_i(z) p_i(\bar{v}_s, u^k_{i,\max},\ \xi^k) \\
\frac{d\bar{w}_i}{dt} &= \bar{f}_{s_i}(\bar{w}_i, [\bar{v}_s]^i) + \mathcal{P}_{s_i}\mathcal{T}^k_s\mathcal{P}_s b^k_i(z) p_i(\bar{w}_i, [\bar{v}_s]^i, u^k_{i,\max},\ \xi^k) \\
\frac{dv_{s_j}}{dt} &= \bar{f}_{s_j}(\bar{v}_s) + \mathcal{P}_{s_j}\mathcal{T}^k_s\mathcal{P}_s b^k_j(z)[p_j(\bar{v}_s, u^k_{j,\max},\ \xi^k) + f^k_{a_j}], \\
&\qquad j = 1, \ldots, m, \quad j \neq i
\end{aligned}
\tag{32}
$$

Note that since $w_i(0) = v_{s_i}(0)$, the states $\overline{w}_i$ and $\overline{v}_{s_i}$, in the earlier system are identical. From Assumption 4, and the fact that $\bar{v} = \mathcal{T}^k\overline{x}_s$, where $\mathcal{T}^k_s$ is an invertible bounded operator, we have that there exists a positive real number, $\delta^k_{v_i} := \|\mathcal{T}^k\|\delta^k_{b_i}$, such that $\|\overline{v}_s(t)\| \leq \delta^k_{v_i}$, for all $t \in [0, T^k_{r_i}]$, that is, the states of the reduced closed-loop system are bounded on a finite time-interval. Using this, and the fact that the fast subsystem is globally exponentially stable, one can show (using calculations similar to those in the Proof of Theorem 9.1 in[54] that given the set of positive real numbers $\{\delta^k_s$, δ^k_f, $\delta_{d_i}{}^k\}$, where $\delta_s{}^k$ is defined in Proposition 1, and δ^k_f, $\delta_{d_i}{}^k$ are arbitrary, there exists a positive real number $\overline{\varepsilon}$, such that if $\varepsilon \in (0, \overline{\varepsilon}]$, $\|x_s(0)\| \leq \delta^k_s$, $\text{l}x_f(0)\|_2 \leq \delta^k_f$, and $w_i(0) = v_{s_i}(0)$, then for all $t \in [0, T^k_{r_i}]$, we have $\|v_{s_i}(t) - \overline{v}_{s_i}(t)\| \leq \alpha_1\varepsilon$ and $\|w_i(t) - \overline{w}_i(t)\| \leq \alpha_2\varepsilon$, for some $\alpha_1 > 0$ and $\alpha_2 > 0$. Rewriting $r_i(t) = \|w_i(t) - v_{s_i}\| \leq \|w_i(t) - \overline{w}_i(t)\| + \|\overline{w}_i(t) - \overline{v}_{s_i}(t)\| + \|\overline{v}_{s_i}(t) - v_{s_i}(t)\|$, and using the fact that $\|\overline{w}_i(t) - \overline{v}_{s_i}(t)\| = 0$ when $f_{a_i}{}^k = 0$ (from Proposition 1), we have $r_i(t) \leq \|w_i(t) - \overline{w}_i(t)\| + \|\overline{v}_{s_i}(t) - v_{s_i}(t)\| \leq \alpha_3\varepsilon$, for all $t \in [0, T^k_{r_i}]$, where $\alpha_3 = \alpha_1 + \alpha_2$. Therefore, given any $\delta^k_{d_i} > 0$, there exists $\varepsilon' := \min\{\delta^k_{d_i}/\alpha_3, \overline{\varepsilon}\}$, such that for $\varepsilon \leq \varepsilon'$, r_i $(t) \leq \delta^k_{d_i}$ for all $t \in [0, T^k_{r_i}]$. This completes the Proof of Proposition 3.

Proof of Theorem 2: The proof is split into two parts. In the first part, we establish asymptotic stability of the origin of the closed-loop system under the switching rule of Eq. 29. Then, in the second part of the proof, we use this stability result to prove near optimality of the fallback actuator configuration with respect to the cost functional of Eq. 28.

Part 1: Consider first the case when no faults in the i-th actuator are present (that is, $T_{d_i} \rightarrow \infty$). In this case, we have from Eq. 29 that control configuration $k = j$ is implemented for all times. Applying the results of Propositions 2 and 3 with $k = j$, we have that given the set $\{\delta^j_s, \delta^j_f, \delta^j_{d_i}\}$ there exists a positive real number $\varepsilon_1 > 0$, such that if $\varepsilon \leq \varepsilon_1$, $\|x_s(0)\| \leq \delta^j_s$, and $\|x_f\ (0)\|_2 \leq \delta^j_f$, the origin of the closed-loop system is asymptotically (and locally exponentially) stable, and the i-th residual satisfies $r_i(t) \leq \delta^j_{d_i}$ for all $t \in [0, T^j_{r_i}]$. In the case of a fault in the i-th actuator, we know from the definitions of $f^j_{a_i}$ and T_{d_i} that no faults occur for $0 \leq t < T_{d_i}$, and, therefore, Eq. 29 dictates that $k(t) = j$ for $0 \leq t < T_{d_i}$. From the stability of the j-th closed-loop system established in Proposition 2, and the closeness of solutions result in Proposition 3, we have that the slow and fast closed-loop states stay bounded, and that the residual of the i-th filter satisfies $r_i(t) \leq \delta^j_{d_i}$, for $0 \leq t < T_{d_i}$, provided $\varepsilon \leq \varepsilon_1$, $\|x_s(0)\| \leq \delta_s{}^j$, $\|x_f(0)\|_2 \leq \delta_f{}^j$, and $w_i(0) = v_{s_i}(0)$. At time T_{d_i}, the supervisor switches (per Eq. 29) to a control configuration $k = \mu$, for which $\|x_s(T_{d_i})\| \leq \delta^\mu_s$, and continues to implement it in the closed-loop system for all future times $t \geq T_{d_i}$. Since the fast state is also bounded at T_{d_i}, there exists a positive real number δ^μ_f, such that $\|x_f(T_{d_i})\|_2 \leq \delta^\mu_f$. At this point, a second application of the result of Proposition 2, with $k = \mu$, yields the existence of a positive real number $\varepsilon_2 > 0$, such that if $\varepsilon \leq \varepsilon_2$, $\|x_s(T_{d_i})\| \leq \delta_s{}^\mu$, and $\|x_f(T_{d_i})\|_2 \leq \delta^\mu_f$, the origin of the closed-loop system is asymptotically (and locally exponentially) stable.

Part 2: From Part 1, we know that, in the absence of faults, the origin of the closed-loop system under actuator configuration $k = j$ is asymptotically (and locally exponentially) stable for $\varepsilon \leq \varepsilon_1$, $\|x_s(0)\| \leq \delta^j_s$, and $\|x_f(0)\|_2 \leq \delta^j_f$. This implies that given any $T^j_b > 0$, there exists $\varepsilon_3 > 0$ such that, for $\varepsilon \leq \varepsilon_3$, and for all $t \geq T^j_b$, $\|x_s(t;\ x(T^j_b),\ \xi^j) - \overline{x}_s(t;\ x(T^j_b),\ \xi^j)\| \leq \beta_1\varepsilon$ and $\|x_f(t;\ x(T^j_b),\xi^j)\|_2 \leq \beta_2\varepsilon$, for some $\beta_1 > 0$ and $\beta_2 > 0$.

Similarly, from the stability of the closed-loop system under actuator configuration $k = \mu$ for $t \geq T_{d_i}$, we have that, given any $T_b^\mu > 0$, there exists $\varepsilon_4 > 0$, such that, for $\varepsilon \leq \varepsilon_4$, and for all $t \geq T_b^\mu$, $\|x(t;\, x_s(T_b^\mu),\, \xi^\mu) - \bar{x}_s(t;\, x_s(T_b^\mu),\, \xi^\mu)\| \leq \beta_3\varepsilon$ and $\|x_f(t;\, x(T_b^\mu),\, \xi^\mu)\|_2 \leq \beta_4\varepsilon$, for some $\beta_3 > 0$ and $\beta_4 > 0$. Without loss of generality, we choose $T_b^\mu = T_b^j := T_b > T_{d_i}$, and let $\varepsilon \leq \min\{\varepsilon_3, \varepsilon_4\}$. Therefore, we have for all $t \geq T_b^\mu$

$$\begin{aligned}\|e_s(t)-\bar{e}_s(t)\| \leq \|x_s(t,\xi^\mu)-\bar{x}_s(t,\xi^\mu)\|+\|x_s(t,\xi^j)-\bar{x}_s(t,\xi^j)\| \leq \beta_5\varepsilon \\ \|e_f(t)\|_2 \leq \|x_f(t,\xi^\mu)\|_2+\|x_f(t,\xi^j)\|_2 \leq \beta_6\varepsilon \qquad (33)\end{aligned}$$

where $\beta_5 = \beta_1 + \beta_3$ and $\beta_6 = \beta_2 + \beta_4$, and from the continuity property of $p(\cdot)$ with respect to x_s, we have

$$\begin{aligned}|e_u(t) - \bar{e}_u(t)| \;&\leq\; |p(x_s(t),\xi^\mu) - p(\bar{x}_s(t),\xi^\mu)| \\ &+ |p(x_s(t),\xi^j) - p(\bar{x}_s(t),\xi^j)| \;\leq\; \beta_7\varepsilon \qquad (34)\end{aligned}$$

for some $\beta_7 > 0$. Consider now the cost functionals of Eq. 18 and Eq. 28, which can be rewritten, respectively,

$$\begin{aligned}\bar{J}_s(\xi^\mu) &= \int_{T_{d_i}}^{T_b} l(\bar{e}_s(t),\bar{e}_f(t),\bar{e}_u(t))dt + \int_{T_b}^{\infty} l(\bar{e}_s(t),\bar{e}_f(t),\bar{e}_u(t))dt \\ J(\xi^\mu) &= \int_{T_{d_i}}^{T_b} l(e_s(t),e_f(t),e_u(t))dt + \int_{T_b}^{\infty} l(e_s(t),e_f(t),e_u(t))dt \qquad (35)\end{aligned}$$

where $l(e_s,e_f,e_u) = (e_s,Q_se_s)+(e_f,Q_fe_f)+e_u^TRe_u$. From Eqs. 33–34, we have that, as $\varepsilon \to 0$, $e_s(t) \to \bar{e}_s(t)$, $e_f(t) \to 0$ and $e_u(t) \to \bar{e}_u(t)$, for $t \geq T_b^\mu$. This, together with the continuity property of the function l in Eq. 35 with respect to its arguments, implies that $l(e_s,\, e_f,\, e_u) \to l(\bar{e}_s,\, \bar{e}_f,\, \bar{e}_u)$ as $\varepsilon \to 0$ and, therefore

$$\int_{T_b^\mu}^{\infty} l(e_s(t),e_f(t),e_u(t))dt \to \int_{T_b^\mu}^{\infty} l(\bar{e}_s(t),\bar{e}_f(t),\bar{e}_u(t))dt \text{ as } \varepsilon \to 0 \qquad (36)$$

From the stability of the finite-dimensional and infinite-dimensional closed-loop systems under actuator configurations j and μ, it follows that there exist positive real numbers $\overline{M}$ and M, such that $l(\bar{e}_s(t),\, \bar{e}_f(t),\, \bar{e}_u(t)) \leq \overline{M}$ and $l(e_s(t),\, e_f(t),\, e_u(t)) \leq M$, for all $t \geq T_{d_i}$. This, together with the fact that $T_b - T_{d_i} = O(\varepsilon)$, yields

$$\begin{aligned}\int_{T_{d_i}}^{T_b} l(\bar{e}_s(t),\bar{e}_f(t),\bar{e}_u(t))dt &\leq \int_{T_{d_i}}^{T_b} \bar{M}dt \leq \bar{M}\varepsilon \\ \int_{T_{d_i}}^{T_b} l(e_s(t),e_f(t),e_u(t))dt &\leq \int_{T_{d_i}}^{T_b} Mdt \leq M\varepsilon \qquad (37)\end{aligned}$$

which implies that as $\varepsilon \to 0$, $\int_{T_{d_i}}^{T_b} l(\bar{e}_s(t),\, \bar{e}_f(t),\, \bar{e}_u(t))dt \to 0$ and $\int_{T_{d_i}}^{T_b} l(e_s(t),\, e_f(t),\, e_u(t))dt \to 0$. Combining Eqs. 36–37, we conclude that $J(\xi^\mu) \to \overline{J}_s(\xi^\mu)$ as $\varepsilon \to 0$. Choosing $\varepsilon^s{:} = \min\{\varepsilon_1,\, \varepsilon_2,\, \varepsilon_3,\, \varepsilon_4\}$ completes the proof of the theorem.

Manuscript received Aug. 18, 2006, and revision received Mar. 5, 2007.