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

Integrated Fault Diagnosis and Robust Safe-Parking for Fault-Tolerant Control of Nonlinear Systems

Miao Du, Jake Nease and Prashant Mhaskar

Abstract— **In this work, we consider the problem of fault diagnosis and fault-handling for nonlinear systems subject to actuator faults. A model-based fault diagnosis scheme is proposed, which can not only identify the failed actuator, but also estimate the magnitude of the fault. With the aid of the fault diagnosis design, the safe-parking framework for fault-tolerant control is extended to handle the case where an actuator seizes at an arbitrary position. The efficacy of the proposed framework is demonstrated through a chemical reactor example.**

I. Introduction

Automatic control technologies have significantly improved the quality of chemical products and the profitability of chemical plant operations in the past few decades. The increased level of automation, however, also makes the control system vulnerable to equipment abnormalities, such as actuator (e.g., valves and pumps) and senor (e.g., thermocouples and flow meters) faults. These abnormalities can lead to safety hazards and substantial economic losses if they are not properly handled. This realization has motivated significant research efforts on fault detection and isolation (FDI) and fault-tolerant control (FTC) in academic and industrial communities.

For the problem of FDI, the existing results can be divided into data-based [1] and model-based [2], [3] approaches. In this work, we mainly discuss the model-based approach, which has been studied extensively for linear systems [4], [5] and nonlinear systems [6], [7]. In this approach, FDI is often achieved by generating residuals through the system model and input/output data. Under fault-free conditions, these residuals are zero, or converge to zero. A fault is reported when a non-zero residual is generated, or a residual breaches a user-specified threshold. Due to the presence of plant-model mismatch, residuals that are sensitive to faults but insensitive to uncertainty and disturbances are desired. Unknown input observers are developed in [4] to decouple the effect of unknown inputs, such as disturbances, from that of the faults for linear systems. For nonlinear systems, the problem has been studied by using uniform thresholds in [6] (and adaptive thresholds in [7]), where fault isolation relies on the existence of a state variable which is directly and uniquely affected by the potential fault. While there are several results on FDI, relatively less attention has been paid to the problem of fault diagnosis (where the problem is not only to isolate the fault, but also to estimate the magnitude of the fault), in part due to the nature of the FTC techniques described below.

Most of the existing results on fault-handling have addressed the problem of preserving nominal operation in the presence of faults, which can be broadly categorized into passive and active approaches. In the passive approach, the key idea is to design robust/reliable feedback controllers by treating faults as disturbances (e.g., [8]). In the active approach, nominal operation is continued by activating an appropriate backup control configuration, where the failed actuator is not used (e.g., [9]). These methods, however, assume that sufficient control effort is available to maintain operation at the nominal equilibrium point. Furthermore, the reconfiguration-based approach typically assumes that the faulty actuator can be “removed” from the control loop and the control action is reverted to its “nominal” value (thereby not requiring the estimation of the fault magnitude). In many practical cases, however, the failed actuator either reverts to a fail-safe position, which is a built-in position for the control actuator to prevent the occurrence of hazardous situations, or simply seizes at an arbitrary position. In these cases, it is possible that the nominal equilibrium point is no longer an equilibrium point in the presence of faults, and the FTC approaches of [8], [9] may not remain applicable.

To handle faults that preclude the possibility of nominal operation, a safe-parking framework has recently been proposed for an isolated unit [10] and studied in the context of a plant-wide setting [11]. More recently, it has been generalized to handle faults in switched nonlinear systems [12]. The key idea of this approach is to operate the system at an appropriate temporary equilibrium point (which is called a safe-park point) under faulty conditions and resume nominal operation smoothly upon fault repair. These results, however, assume fixed and known fail-safe positions, which do not require knowledge of the fault magnitude. Therefore, it does not remain directly applicable to the case where an actuator seizes at an arbitrary position due to such reasons as mechanical failures or loss of power. For this problem, a fault diagnosis design is required to estimate the position of the failed actuation in order to implement the safe-parking operation.

Motivated by the above considerations, we consider the problem of designing an integrated fault diagnosis and safe-parking framework to handle faults in nonlinear systems. In particular, we consider the case where an actuator seizes at an arbitrary position, and the fault precludes the possibility

Financial support from NSERC and the McMaster Advanced Control Consortium is gratefully acknowledged.

Miao Du, Jake Nease and Prashant Mhaskar are with the Department of Chemical Engineering, McMaster University, Hamilton, ON L8S 4L7, Canada dum4@mcmaster.ca, neasej@mcmaster.ca, mhaskar@mcmaster.ca

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

of nominal operation. The remainder of the manuscript is organized as follows. In Section II, the class of systems considered is presented. In Section III, a model-based fault diagnosis scheme is developed. In Section IV, a robust safe-parking framework is designed to handle actuator faults in nonlinear systems. The efficacy of the proposed framework is demonstrated through a chemical reactor example in Section V. Finally, Section VI presents some concluding remarks.

II. Preliminaries

Consider a nonlinear system subject to actuator faults with the following state-space description:

$$\begin{aligned}
&\dot{x} = f(x,\theta(t)) + G(x)[u(t) + \tilde{u}(t)]\\
&u(t) \in \mathcal{U}, \theta(t) \in \Theta\\
&u(t) + \tilde{u}(t) = u(t_k) + \tilde{u}(t_k) \in \mathcal{U} \text{ for all } t \in [t_k, t_{k+1})\\
&k = 0, \cdots, \infty
\end{aligned} \tag{1}$$

where $x = [x_1, \cdots, x_n]^{\mathrm{T}} \in \mathbb{R}^n$ is the vector of state variables, $u = [u_1, \cdots, u_m]^{\mathrm{T}} \in \mathbb{R}^m$ is the vector of prescribed control inputs given by the control law and $\tilde{u} = [\tilde{u}_1, \cdots, \tilde{u}_m]^{\mathrm{T}} \in \mathbb{R}^m$ is the unknown fault vector for the actuators, with the actual control input $u + \tilde{u}$ implemented to the plant taking values in a nonempty compact convex set $\mathcal{U} := \{u \in \mathbb{R}^m : u_{\min} \leq u \leq u_{\max}\}$ that contains 0, where $u_{\min} = [u_{1,\min}, \cdots, u_{m,\min}]^{\mathrm{T}}$, $u_{\max} = [u_{1,\max}, \cdots, u_{m,\max}]^{\mathrm{T}} \in \mathbb{R}^m$ denote the lower and upper bounds (constraints) on the vector of manipulated variables, respectively, and $\theta = [\theta_1, \cdots, \theta_q]^{\mathrm{T}} \in \mathbb{R}^q$ is the vector of (possibly time-varying) uncertain variables taking values in a nonempty compact convex set $\Theta = \{\theta \in \mathbb{R}^q : \theta_{\min} \leq \theta \leq \theta_{\max}\}$ that contains 0, where $\theta_{\min} = [\theta_{1,\min} \cdots, \theta_{q,\min}]^{\mathrm{T}}$, $\theta_{\max} = [\theta_{1,\max}, \cdots, \theta_{q,\max}]^{\mathrm{T}} \in \mathbb{R}^q$ denote the lower and upper bounds on the vector of uncertain variables, respectively. It is assumed that the functions $f(\cdot,\cdot) = [f_i(\cdot,\cdot)]_{n\times 1}$ and $G(\cdot) = [g_{ij}(\cdot)]_{n\times m}$ ($i = 1, \cdots, n$; $j = 1, \cdots, m$) are locally Lipschitz. The origin is an equilibrium point for the nominal system (the system of Eq. (1) with $\tilde{u}(t) \equiv 0$ and $\theta(t) \equiv 0$) for $u = 0$, i.e., $f(0,0) = 0$. The control input is prescribed at discrete times $t_k := k\Delta$, $k = 0, \cdots, \infty$, where Δ denotes the period during which the control action is constant. We consider faults such that an actuator seizes at an arbitrary position. It is assumed that the corrupted input to the plant is constant during each time interval, that is, $u(t)+\tilde{u}(t) = u(t_k)+\tilde{u}(t_k)$ for all $t \in [t_k, t_{k+1})$. Throughout the manuscript, the notation $L_f h(\cdot)$ denotes the standard Lie derivative of a scalar function $h(\cdot)$ with respect to a vector function $f(\cdot)$ and $\|\cdot\|$ denotes the Euclidean norm. Note that $-u_{i,\min}$ (or $-\theta_{i,\min}$) does not have to be equal to $u_{i,\max}$ (or $\theta_{i,\max}$), $i = 1, \cdots, q$. In this work, the Lyapunov-based predictive control design of [13] under Assumption 1 below is used to illustrate the proposed methodology.

Assumption 1: For the system of Eq. (1), $f_i(x,\theta)$, $i = 1, \cdots, n$, is monotonic with respect to θ_j, $j = 1, \cdots, q$, for any $x \in \mathbb{R}^n$ and $\theta_l \in [\theta_{l,\min}, \theta_{l,\max}]$, $l = 1, \cdots, q$ and $l \neq j$.

Remark 1: In many practical systems, the form of $f(x,\theta)$ is known and the uncertain variables affect $f(x,\theta)$ monotonically, as required in Assumption 1. For example, in chemical processes the reaction rate is monotonically increasing with respect to the pre-exponential constant, while the rate of heat generated by the reaction is monotonically decreasing with respect to the enthalpy of the reaction. While Assumption 1 is used to present the methodology, it should be noted that a more general assumption can be stated as follows: there exist known functions $f_l(x)$ and $f_u(x)$ such that $f_l(x) \leq f(x,\theta) \leq f_u(x)$ for all $\theta \in \Theta$.

Consider the system of Eq. (1) under fault-free conditions, for which a control Lyapunov function $V(x)$ exists and Assumption 1 holds. Let Π denote a set of states where $\dot{V}(x(t))$ can be made negative by using the allowable values of the constrained input:

$$\begin{aligned}
\Pi =\{x \in \mathbb{R}^n : &\sup_{\theta\in\Theta} L_f V(x,\theta) + \inf_{u\in\mathcal{U}} L_G V(x)u\\
&\leq -\varepsilon V(x)\}
\end{aligned} \tag{2}$$

where $L_G V(x) = [L_{g_1} V(x), \cdots, L_{g_m} V(x)]$, with g_i the ith column of G, and ε is a positive real number. It is assumed that $L_f V(x,\theta)$ and $L_G V(x)$ are locally Lipschitz. The robust controller of [13] possesses a stability region, an estimate of which is given by:

$$\{x \in \Pi : V(x) \leq c\} \tag{3}$$

where c is a positive (preferably the largest possible) constant. To estimate the upper bound on $L_f V(x,\theta)$, let $\theta_{i,l} = [\theta_{i,1,l}, \cdots, \theta_{i,q,l}]$, $\theta_{i,u} = [\theta_{i,1,u}, \cdots, \theta_{i,q,u}]$, $i = 1, \cdots, n$, where $\theta_{i,j,l} = \begin{cases} \theta_{j,\max}, & \text{if } \frac{df_i}{d\theta_j} \leq 0 \\ \theta_{j,\min}, & \text{if } \frac{df_i}{d\theta_j} > 0 \end{cases}$, $\theta_{i,j,u} = \begin{cases} \theta_{j,\min}, & \text{if } \frac{df_i}{d\theta_j} \leq 0 \\ \theta_{j,\max}, & \text{if } \frac{df_i}{d\theta_j} > 0 \end{cases}$, $j = 1, \cdots, q$. Note that $\theta_{i,l}$ and $\theta_{i,u}$ are the instances of θ that make $f_i(x,\theta)$ take its minimum and maximum values for given x, respectively. Let $\theta_{f_i} = \begin{cases} \theta_{i,l}, & \frac{\partial V}{\partial x_i} \leq 0 \\ \theta_{i,u}, & \frac{\partial V}{\partial x_i} > 0 \end{cases}$, $i = 1, \cdots, n$. It follows that $\sum_{i=1}^{n} \frac{\partial V}{\partial x_i} f_i(x,\theta_{f_i})$ is an estimate of the upper bound on $L_f V(x,\theta)$, and $\inf_{u\in\mathcal{U}} L_G V(x)u$ can be computed in a similar way. Note that while the control law of [13] is used as an example of a control design for illustration, the proposed results hold under any control law (which we refer to as $RC(x)$) that satisfies Assumption 2 below.

Assumption 2: For the system of Eq. (1) under fault-free conditions, there exist a robust control law $RC(x)$ and a set $\Omega \in \mathbb{R}^n$ such that given any positive real number d, there exist positive real numbers Δ^* and T such that if $\Delta \in (0, \Delta^*]$ and $x(0) \in \Omega$, then $x(t) \in \Omega$ for all $t \geq 0$ and $\|x(t)\| \leq d$ for all $t \geq T$.

III. Fault detection and diagnosis structure

In this section, under the assumption of full state feedback, we design an FDI scheme using constant thresholds and then, for a special case, devise a fault detection and diagnosis (FDD) scheme using time-varying thresholds. With the assumption that $m \leq n$, the system of Eq. (1) can be decomposed into two coupled subsystems: what we denote as a diagnosable subsystem and the remainder of the original system, with states denoted by $x_d \in \mathbb{R}^m$ and $x_{\bar{d}} \in \mathbb{R}^{n-m}$, respectively. Accordingly, we have $f(x, \theta) = [f_d(x, \theta)^{\mathrm{T}}, f_{\bar{d}}(x, \theta)^{\mathrm{T}}]^{\mathrm{T}}$ and $G(x, \theta) = [G_d(x)^{\mathrm{T}}, G_{\bar{d}}(x)^{\mathrm{T}}]^{\mathrm{T}}$. The system of Eq. (1) can then be written as follows:

$$\dot{x}_d = f_d(x, \theta) + G_d(x)[u(t) + \tilde{u}(t)] \tag{4a}$$

$$\dot{x}_{\bar{d}} = f_{\bar{d}}(x, \theta) + G_{\bar{d}}(x)[u(t) + \tilde{u}(t)] \tag{4b}$$

The key idea of the proposed methodology is to construct input-based residuals by utilizing the system model and state measurements. To this end, consider the time interval $[t_k, t_{k+1})$. Integrating both sides of Eq. (4a) over $[t_k,\, t_{k+1})$ gives the following equation:

$$\begin{aligned} x_d(t_{k+1}) &= x_d(t_k) + \int_{t_k}^{t_{k+1}} \{f_d(x, \theta) \\ &\quad + G_d(x)[u(t) + \tilde{u}(t)]\}dt \\ &= x_d(t_k) + F_{d,k} + G_{d,k}[u(t_k) + \tilde{u}(t_k)] \end{aligned} \tag{5}$$

where $F_{d,k} = \int_{t_k}^{t_{k+1}} f_d(x, \theta)dt$ and $G_{d,k} = \int_{t_k}^{t_{k+1}} G_d(x)dt$. The system of Eq. (1) has a diagnosable subsystem of Eq. (4a) if it satisfies Assumption 3 below.

Assumption 3: For the system of Eq. (1), $m \leq n$ and $G_{d,k}$ is invertible for $k = 0, \cdots, \infty$.

Remark 2: To illustrate the idea behind Assumption 3, consider a scalar system described by $\dot{x} = x + u_1 + 2u_2$, where $x,\, u_1,\, u_2 \in \mathbb{R}$. For this system, it is impossible to differentiate the fault between u_1 and u_2, because the number of state variables is eclipsed by that of the input variables (i.e., $m > n$). It is also possible that inputs affect states in the same manner through different channels. For example, fault isolation is impeded in the system described by $\dot{x} = x + \left[\begin{smallmatrix} 1 & 1 \\ 2 & 2 \end{smallmatrix}\right] u$, where $x,\, u \in \mathbb{R}^2$. A simple example of a diagnosable system is given by $\dot{x} = x + \left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right] u$, where x, $u \in \mathbb{R}^2$, which satisfies Assumption 3.

Remark 3: To allow fault isolation, it is assumed in [6] that for every input u_j, $j = 1, \cdots, m$, there exists a state x_i, $i \in \{1, \cdots, n\}$ such that with x_i as an output, the relative degree of x_i with respect to u_j and only with respect to u_j is equal to 1. Under this assumption, $G_d(x)$ is a diagonal matrix with non-zero elements on its diagonal and is therefore invertible. Assumption 3, however, only requires that $G_{d,k}$ is invertible, and $G_d(x)$ could be a non-diagonal matrix.

Let $[G_{d,k}^{-1}]_i$ denote the ith row of $G_{d,k}^{-1}$. For $i = 1, \cdots, m$, define the residuals as

$$r_{i,k} = |[G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k) - \bar{F}_{d,k}] - u_i(t_k)| \tag{6}$$

where $\bar{F}_{d,k} = \int_{t_k}^{t_{k+1}} f_d(x, 0)dt$. Note that $[G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k) - \bar{F}_{d,k}]$ is the estimate of the actual input to the plant by using the nominal model. It follows from Eq. (5) that

$$u_i(t_k) + \tilde{u}_i(t_k) = [G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k) - F_{d,k}] \tag{7}$$

Substituting $u_i(t_k)$ in Eq. (7) into Eq. (6) gives $r_{i,k} = |[G_{d,k}^{-1}]_i(F_{d,k} - \bar{F}_{d,k}) + \tilde{u}_i(t_k)|$. The FDI scheme using constant thresholds is formalized in Theorem 1 below.

Theorem 1: Consider the system of Eq. (1), for which Assumption 3 holds. Assume $\|[G_{d,k}^{-1}]_i\| \leq K_{g,i}$ for $k = 0, \cdots, \infty$, where $K_{g,i}$ is a positive real number. Then, there exists $\delta_i > 0$ such that if $r_{i,k} > \delta_i$, then $\tilde{u}_i(t_k) \neq 0$.

Proof: Since the vector function $f_d(x, \theta)$ is locally Lipschitz, there exists $K_f > 0$ such that

$$\|f_d(x, \theta) - f_d(x, 0)\| \leq K_f \theta_b \tag{8}$$

where $\theta_b = \|[\max\{-\theta_{1,\min},\, \theta_{1,\max}\},\, \cdots,\, \max\{-\theta_{q,\min},\, \theta_{q,\max}\}]^{\mathrm{T}}\|$. If $\tilde{u}_i(t_k) = 0$, it follows that

$$\begin{aligned} r_{i,k} &= |[G_{d,k}^{-1}]_i(F_{d,k} - \bar{F}_{d,k})| \\ &= |[G_{d,k}^{-1}]_i \int_{t_k}^{t_{k+1}} [f_d(x, \theta) - f_d(x, 0)]dt| \\ &\leq K_{g,i} K_f \theta_b \Delta \end{aligned} \tag{9}$$

It means that for $\delta_i = K_{g,i} K_f \theta_b \Delta$, if $\tilde{u}_i(t_k) = 0$, then $r_{i,k} \leq \delta_i$. Therefore, if $r_{i,k} > \delta_i$, then $\tilde{u}_i(t_k) \neq 0$. This concludes the proof of Theorem 1. ■

Remark 4: Theorem 1 shows that there exists a uniform bound on the error between the estimate of the input to the plant and the prescribed control input, $u_i(t_k)$, for each manipulated variable. The result establishes a sufficient condition for FDI: if the bound is breached, then an actuator fault must have taken place. The design allows for "small" faults, which are indistinguishable from the effect of the system uncertainty, to go undetected; however, such faults, since they essentially have the same effect as the system uncertainty, may be handled by the robustness of the control design.

Remark 5: It is assumed in Theorem 1 that $\|[G_{d,k}^{-1}]_i\|$ is bounded, which is necessary for the proposed method to detect and isolate faults. It should be noted, however, that if this assumption is not satisfied, one possibility is that the impact of the input on the system state evolution is negligible. Consequently, even if a fault takes place, it may not affect the system significantly. When the system goes to a region where the effect of the control action on the system becomes significant again, the proposed method can effectively detect and isolate faults.

We also consider a special case where time-varying bounds (in the discrete-time domain) on the outputs of the actuators can be used for FDD. To this end, we first derive bounds on $F_{d,k}$ under Assumption 1. Define $\theta_{d,i,l}$ and $\theta_{d,i,u}$ in the same way as $\theta_{i,l}$ and $\theta_{i,u}$ were defined in Section II, for $i = 1, \cdots, m$. Let $f_{d,i}(\cdot, \cdot)$ and $F_{d,i,k}$ denote the ith element of $f_d(\cdot, \cdot)$ and $F_{d,k}$, respectively. It follows that

$$\int_{t_k}^{t_{k+1}} f_{d,i}(x, \theta_{d,i,l})dt \leq F_{d,i,k} \leq \int_{t_k}^{t_{k+1}} f_{d,i}(x, \theta_{d,i,u})dt \tag{10}$$

Let $f_{d,i,k,l} = \int_{t_k}^{t_{k+1}} f_{d,i}(x, \theta_{d,i,l})dt$ and $f_{d,i,k,u} = \int_{t_k}^{t_{k+1}} f_{d,i}(x, \theta_{d,i,u})dt$ denote the lower and upper bounds on $F_{d,i,k}$, respectively. The FDD scheme that uses time-varying bounds on the outputs of actuators is formalized in Theorem 2 below.

Theorem 2: Consider the system of Eq. (1), for which Assumptions 1 and 3 hold. There exist $u_{i,k,l}$ and $u_{i,k,u}$

such that if $u_i(t_k) \notin [u_{i,k,l}, u_{i,k,u}]$, then $\tilde{u}_i(t_k) \neq 0$, and $u_i(t_k) + \tilde{u}_i(t_k) \in [u_{i,k,l}, u_{i,k,u}]$.

Proof: It follows from Eq. (7) that

$$\begin{aligned} u_i(t_k) + \tilde{u}_i(t_k) \geq [G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k)] \\ - \sum_{j=1}^{m} [G_{d,k}^{-1}]_{ij} F_{d,j,k,l} \end{aligned} \tag{11}$$

where $[G_{d,k}^{-1}]_{ij}$ denotes the jth element of $[G_{d,k}^{-1}]_i$ and $F_{d,j,k,l} = \begin{cases} f_{d,j,k,l}, & \text{if } [G_{d,k}^{-1}]_{ij} \leq 0 \\ f_{d,j,k,u}, & \text{if } [G_{d,k}^{-1}]_{ij} > 0 \end{cases}$, $j = 1, \cdots, m$. Let $F_{d,k,l} = [F_{d,1,k,l}, \cdots, F_{d,m,k,l}]^{\mathrm{T}}$. Then, we have that

$$u_i(t_k) + \tilde{u}_i(t_k) \geq u_{i,k,l} \tag{12}$$

where $u_{i,k,l} = [G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k) - F_{d,k,l}]$. Similarly, letting $F_{d,k,u} = [F_{d,1,k,u}, \cdots, F_{d,m,k,u}]^{\mathrm{T}}$, where $F_{d,j,k,u} = \begin{cases} f_{d,j,k,u}, & \text{if } [G_{d,k}^{-1}]_{ij} \leq 0 \\ f_{d,j,k,l}, & \text{if } [G_{d,k}^{-1}]_{ij} > 0 \end{cases}$, $j = 1, \cdots, m$, we have that

$$u_i(t_k) + \tilde{u}_i(t_k) \leq u_{i,k,u} \tag{13}$$

where $u_{i,k,u} = [G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k) - F_{d,k,u}]$. It follows that $u_{i,k,l} \leq u_i(t_k) + \tilde{u}_i(t_k) \leq u_{i,k,u}$, and $u_{i,k,l} \leq u_i(t_k) \leq u_{i,k,u}$ if $\tilde{u}_i(t_k) = 0$. Therefore, $u_i(t_k) \notin [u_{i,k,l}, u_{i,k,u}]$ implies that $\tilde{u}_i(t_k) \neq 0$. This concludes the proof of Theorem 2. ■

Remark 6: Theorem 2 uses information about the monotonic nature of the effect of uncertainty on the state evolution to generate time-varying bounds on the implemented control action. In particular, in the absence of faults, the implemented control action equals the prescribed control action, and therefore the prescribed control input should reside within the bounds on the implemented control action for each manipulated variable. If the prescribed control action breaches these bounds for some manipulated variable, the only way that can happen is when the implemented control action is no longer equal to the prescribed control action for the same manipulated variable, resulting in the detection and isolation of the fault. Note that beyond FDI, the fault diagnosis scheme provides an estimate of the output of the failed actuator.

The FDD procedure for the case where an actuator seizes at an arbitrary position is summarized as follows:

1) At time t_{k+1}, $k = 0, \cdots, \infty$, compute $u_{i,k,l}$ and $u_{i,k,u}$, $i = 1, \cdots, m$.
2) Let

$$r_{b,i}(k) := \begin{cases} 1, & \text{if } u_i(t_k) \notin [u_{i,k,l}, u_{i,k,u}] \\ 0, & \text{otherwise} \end{cases} \tag{14}$$

where $r_{b,i}(k)$ denotes a binary residual. If n_d non-zero residuals $r_{b,i}$ are monitored successively, where n_d is a design parameter, report a fault at time $t_d = t_{k+1}$ for the actuator that corresponds to u_i and choose $\bar{u}_{i,l} = \max \cup_{j \in \{k+1-n_d, \cdots, k\}} \{u_{i,j,l}\} \cup \{u_{i,\min}\}$ and $\bar{u}_{i,u} = \min \cup_{j \in \{k+1-n_d, \cdots, k\}} \{u_{i,j,u}\} \cup \{u_{i,\max}\}$ as the lower and upper bounds on the failed actuator position, respectively. Otherwise, repeat Step 1.

IV. Robust safe-parking for fault-tolerant control

In this section, we consider the problem of fault-handling for the case where an actuator seizes at an arbitrary position (and does not revert to the pre-designed fail-safe position). The key idea of the proposed approach is to design several safe-park point candidates off-line for a finite number of potential failed actuator positions, and upon FDD, choose a safe-park point on-line such that the system can be stabilized at the chosen safe-park point by the robust control law, which can handle the error between the actual failed actuator position and its design counterpart.

Specifically, we design safe-park point candidates for M possible actuator positions of u_i denoted by $\bar{u}_{s,i,j} \in [u_{i,\min}, u_{i,\max}]$, $j = 1, \cdots, M$. When designing the control law and characterizing the stability region of a safe-park point candidate, a design uncertain variable of magnitude δ_s (over and above the uncertain variables in the system description), is used to account for the possible error between the actual value of the failed actuator position, denoted by $\bar{u}_{i,f}$, and the one used to design the safe-park point candidate ($\bar{u}_{s,i,j}$). Let u_{nom} and $u_{s,i,j}$ denote the control laws to stabilize the system at the nominal equilibrium point x_{nom} and a safe-park point candidate $x_{s,i,j}$, respectively, yielding Ω_{nom} and $\Omega_{s,i,j}$ as their stability regions. The safe-parking framework is formalized in Theorem 3 below.

Theorem 3: Consider the system of Eq. (1) under a control law $RC(x)$ satisfying Assumption 2. Let t_f be the time when a fault takes place, t_d the time when it is detected and diagnosed, and t_r the time when it is repaired. For $x(0) \in \Omega_{nom}$, if $[\bar{u}_{i,l}, \bar{u}_{i,u}] \subseteq [\bar{u}_{s,i,j} - \delta_s, \bar{u}_{s,i,j} + \delta_s]$, $x(t_d) \in \Omega_{s,i,j}$, and $B_{d,s,i,j} \subseteq \Omega_{nom}$, then the switching rule

$$u(t) = \begin{cases} u_{nom}(t), & 0 \leq t < t_d \\ u_{s,i,j}(t), & t_d \leq t < t_e \\ u_{nom}(t), & t_e \leq t \end{cases} \tag{15}$$

where $B_{d,s,i,j}$ is a closed ball of radius d around $x_{s,i,j}$ and $t_e \geq t_r$ is such that $x(t_e) \in \Omega_{nom}$, guarantees that $x(t) \in \Omega_{nom}$ $\forall\, t \in [0, t_f] \cup [t_e, \infty)$ and there exists a positive real number T such that $\|x(t)\| \leq d$ for all $t \geq T$.

Remark 7: Upon confirmation of the fault, the safe-parking mechanism described by Theorem 3 is activated to shift the control objective from operating the system at the nominal equilibrium point to maintaining it at a suboptimal but admissible operating point. Note that a safe-park point is chosen from the candidates for the design value of the failed actuator position $\bar{u}_{s,i,j}$ such that the range $[\bar{u}_{s,i,j} - \delta_s, \bar{u}_{s,i,j} + \delta_s]$ designed off-line contains the range $[\bar{u}_{i,l}, \bar{u}_{i,u}]$ identified on-line for the estimate of the failed actuator position, as illustrated in Fig. 1. Since $[\bar{u}_{i,l}, \bar{u}_{i,u}]$ contains the actual value of the failed actuator position $\bar{u}_{i,f}$, it is guaranteed that such a safe-park point candidate is a feasible equilibrium point subject to the fault. Note also that an arbitrarily chosen safe-park point candidate is not guaranteed to be a feasible equilibrium point in the presence of the fault.

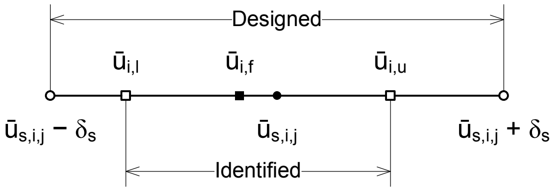


Fig. 1. Schematic illustrating the choice of the safe-park point. The range $[\bar{u}_{s,i,j}-\delta_s, \bar{u}_{s,i,j}+\delta_s]$ is designed off-line for the actuator position $\bar{u}_{s,i,j}$ with the robustness margin δ_s. The range $[\bar{u}_{i,l}, \bar{u}_{i,u}]$ is identified on-line, which contains the actual value of the failed actuator position $\bar{u}_{i,f}$.

TABLE I

SAFE-PARK POINT CANDIDATES FOR THE CHEMICAL REACTOR EXAMPLE.

Point	Q_c (10^4 kJ/hr)	C_{A} (kmol/m^3)	T_R (K)
S_1	-6.55 ± 1.25	3.50	380
S_2	-5.73 ± 1.25	3.85	375
S_3	-4.91 ± 1.25	3.50	380
S_4	-4.10 ± 1.25	3.50	375
S_5	-3.28 ± 1.25	3.50	375
S_6	-2.46 ± 1.25	3.85	375

Remark 8: The remaining conditions dictating the choice of a safe-park point follow from the safe-parking framework designed for a fail-safe position in [10]. In particular, to make sure that the system can be driven to the temporary operating point, it requires that the system state should reside within the stability region of the safe-park point at the time of fault confirmation. Note that t_e denotes a time when the system state is within the stability region of the nominal equilibrium point after the fault is repaired. If the system state is already within the stability region of the nominal equilibrium point at the time of fault repair, then $t_e = t_r$. Otherwise, the control action is implemented to drive the system state to the safe-park point until it reaches the stability region of the nominal equilibrium point. Then, nominal operation is resumed at time t_e.

V. SIMULATION EXAMPLE

In this section, we illustrate the proposed fault diagnosis techniques and the generalized safe-parking framework via a continuous-stirred tank reactor (CSTR) example, where three parallel irreversible elementary exothermic reactions of the form A $\xrightarrow{k_1}$ B, A $\xrightarrow{k_2}$ U, and A $\xrightarrow{k_3}$ R take place, with A as the reactant species, B the desired product, and U and R the undesired byproducts. The feed to the reactor consists of reactant A at a flow rate F, concentration C_{A0}, and temperature T_{A0}. Under standard assumptions, the mathematical model of the process can be derived from material and energy balances, which takes the following form:

$$\begin{aligned} \dot{C}_{\text{A}} &= \frac{F}{V}(C_{\text{A0}} - C_{\text{A}}) - \sum_{i=1}^{3} R_i(C_{\text{A}}, T_R) \\ \dot{T}_R &= \frac{F}{V}(T_{\text{A0}} - T_R) + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_p} R_i(C_{\text{A}}, T_R) + \frac{Q}{\rho c_p V} \end{aligned} \tag{16}$$

where $R_i(C_{\text{A}}, T_R) = k_i e^{-E_i/RT_R} C_{\text{A}}$ for $i = 1, 2, 3$, C_{A} is the concentration of species A in the reactor, T_R is the temperature of the reactor, Q is the rate of heat added to/removed from the reactor, V is the volume of the reactor, k_i, E_i, and ΔH_i are the pre-exponential constant, the activation energy, and the enthalpy of reaction i, respectively, and c_p and ρ are the heat capacity and density of the reacting mixture, respectively. Under fault-free conditions, the control objective is to stabilize the reactor at the unstable equilibrium point $N(3.50$ kmol/m^3, 405.0 K$)$ by manipulating C_{A0} and Q, where $0 \leq C_{\text{A0}} \leq 6$ kmol/m^3 and -8×10^5 kJ/hr $\leq Q \leq 8 \times 10^5$ kJ/hr. The manipulated variable $Q = Q_c + Q_h$, where Q_c and Q_h denote cooling and heating, respectively, with -8×10^5 kJ/hr $\leq Q_c \leq 0$ and $0 \leq Q_h \leq 8 \times 10^5$ kJ/hr. The nominal steady-state values of the manipulated variables are $C_{\text{A0}} = 4.25$ kmol/m^3 and $Q = -6.55 \times 10^4$ kJ/hr. The simulations are conducted under a 0.5% error in the pre-exponential constant (k_1) for the main reaction and sinusoidal disturbance in the temperature (T_{A0}) of the feed with an amplitude of 3 K and a period of 0.1 hr. The error bounds on k_1 and T_{A0} used in the monitoring and control design are $\pm 1.5\%$ and ± 5 K, respectively. The concentration and temperature measurements are assumed to have a truncated gaussian noise with a standard deviation of 0.01 kmol/m^3 and 0.1 K for the parent normal distribution, respectively. The lower and upper truncation points are -0.02 koml/m^3 and 0.02 koml/m^3 for the concentration, and -0.2 K and 0.2 K for the temperature, respectively. The noisy measurements are filtered before performing fault diagnosis and computing the control input.

To demonstrate the efficacy of the fault diagnosis and safe-parking framework, we consider a failure in the actuator used to control Q_c. The safe-park point candidates are shown in Table I for 6 actuator positions of Q_c with a robustness margin $\delta_s = 1.25 \times 10^4$ kJ/hr. To account for measurement noise, the upper and lower bounds on the estimates of C_{A0} and Q implemented to the plant are relaxed by a magnitude of 0.32 kmol/m^3 and 1848 kJ/hr (inferred from process data under healthy conditions), respectively. In the control law of [13], an execution time $\Delta = 0.025$ hr $= 1.5$ min and a prediction horizon of 2Δ are used. The Lyapunov function used to characterize the stability region and to prescribe the control input for the nominal equilibrium point is chosen as $V(x) = x^{\text{T}}Px$, where $P = \begin{bmatrix} 7.72\times10^{-1} & 0 \\ 0 & 4\times10^{-4} \end{bmatrix}$.

Consider the case where the process starts from an initial condition at $(C_{\text{A}}, T_R) = (2.50$ kmol/m^3, 405.0 K$)$, denoted by O in Fig 2. The actuator fails at time $t_f = 0.05$ hr when the process state is at $F(2.78$ kmol/m^3, 396.1 K$)$. The output value of the failed actuator is $\bar{u}_f = -4.19 \times 10^4$ kJ/hr (the same as it was at time t_f^-) during fault repair. The FDD scheme can be explained by Fig. 3, where the prescribed inputs are marked by crosses, the actual inputs marked by circles, and the estimated bounds on the actual inputs marked by error bars. It can be seen that the fault in Q_c is first declared at 0.1 hr (i.e., there is a two-step time

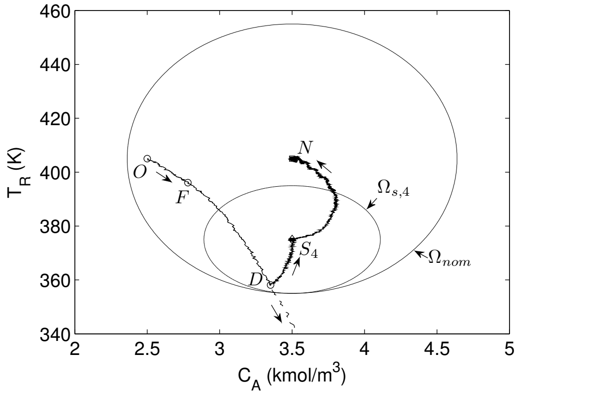
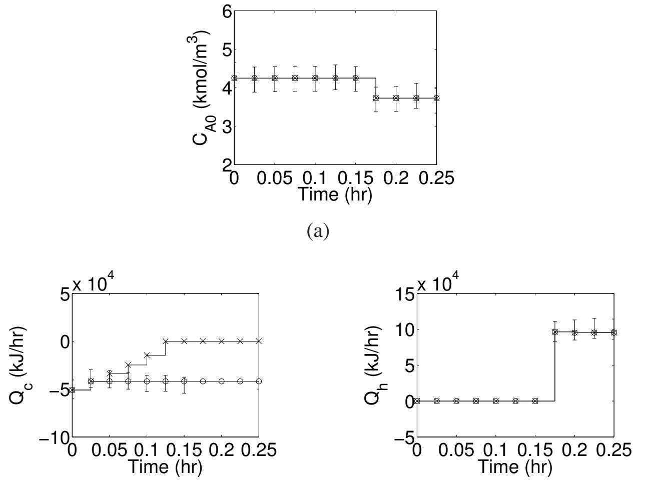


Fig. 2. Closed-loop state trajectories for the chemical reactor example.

delay). Upon the first alarm, the actuator for Q_h is disabled (i.e., the prescribed value of Q_h is 0) to allow FDD for Q_c until the fault is confirmed to be true or false. The fault is confirmed at time $t_d = 0.175$ hr after 4 consecutive alarms, with the process state at $D(3.35$ kmol/m^3, 358.1 K). The binary residuals for the manipulated variables $C_{\rm A0}$ and Q are shown in Figs. 4(a) and 4(b), respectively. Beyond FDI, the identified lower and upper bounds on Q_c are -5.00×10^4 kJ/hr and -3.81×10^4 kJ/hr, respectively. This information is then used to choose a safe-park point. By referring to Table I, it is found that the safe-park point candidate $S_4(3.50$ kmol/m^3, 375 K) is designed for the case where the cooling valve seizes at some value in $[-5.35 \times 10^4$ kJ/hr, -2.85×10^4 kJ/hr], which contains $[-5.00 \times 10^4$ kJ/hr, -3.81×10^4 kJ/hr]. Note also that the process state at time t_d is within the stability region ($\Omega_{s,4}$) of S_4. Therefore, S_4 is chosen as the safe-park point. As shown by the solid trajectory in Fig. 2, if the safe-parking strategy is implemented, the process is first stabilized at S_4, and nominal operation is resumed upon fault repair. The absence of an appropriately designed fault-handling framework, however, results in process instability, as shown by the dashed trajectory in Fig. 2.

VI. Conclusions

In this work, we considered the problem of fault diagnosis and fault-handling for nonlinear systems subject to actuator faults. A model-based fault diagnosis scheme was proposed, which can not only identify the failed actuator, but also estimate the magnitude of the fault. With the aid of the fault diagnosis design, the safe-parking framework for FTC was extended to handle the case where an actuator seizes at an arbitrary position. The efficacy of the proposed framework was demonstrated through a chemical reactor example.

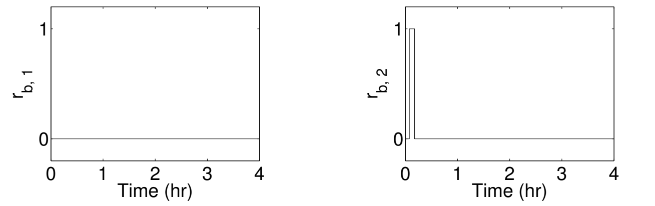


(a)

(b)

(c)

Fig. 3. Illustration of the FDD scheme of Theorem 2 for the chemical reactor example.



(a)

(b)

Fig. 4. Binary residuals for manipulated variables $C_{\rm A0}$ (a) and Q (b), respectively, in the chemical reactor example.

References

[1] V. Venkatasubramanian, R. Rengaswamy, S. N. Kavuri, and K. Yin, "A review of process fault detection and diagnosis Part III: Process history based methods," *Comp. & Chem. Eng.*, vol. 27, pp. 327–346, 2003.

[2] P. M. Frank, "Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results," *Automatica*, vol. 26, pp. 459–474, 1990.

[3] V. Venkatasubramanian, R. Rengaswamy, K. Yin, and S. N. Kavuri, "A review of process fault detection and diagnosis Part I: Quantitative model-based methods," *Comp. & Chem. Eng.*, vol. 27, pp. 293–311, 2003.

[4] J. Chen, R. J. Patton, and H.-Y. Zhang, "Design of unknown input observers and robust fault detection filters," *Int. J. Contr.*, vol. 63, pp. 85–105, 1996.

[5] F. Hamelin and D. Sauter, "Robust fault detection in uncertain dynamic systems," *Automatica*, vol. 36, pp. 1747–1754, 2000.

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

[7] X. Zhang, M. M. Polycarpou, and T. Parisini, "Fault diagnosis of a class of nonlinear uncertain systems with Lipschitz nonlinearities using adaptive estimation," *Automatica*, vol. 46, pp. 290–299, 2010.

[8] Z. D. Wang, B. Huang, and H. Unbehauen, "Robust reliable control for a class of uncertain nonlinear state-delayed systems," *Automatica*, vol. 35, pp. 955–963, 1999.

[9] P. Mhaskar, "Robust model predictive control design for fault-tolerant control of process systems," *Ind. & Eng. Chem. Res.*, vol. 45, pp. 8565–8574, 2006.

[10] R. Gandhi and P. Mhaskar, "Safe-parking of nonlinear process systems," *Comp. & Chem. Eng.*, vol. 32, pp. 2113–2122, 2008.

[11] ——, "A safe-parking framework for plant-wide fault-tolerant control," *Chem. Eng. Sci.*, vol. 64, pp. 3060–3071, 2009.

[12] M. Du and P. Mhaskar, "A safe-parking and safe-switching framework for fault-tolerant control of switched nonlinear systems," *Int. J. Contr.*, vol. 84, pp. 9–23, 2011.

[13] M. Mahmood, R. Gandhi, and P. Mhaskar, "Safe-parking of nonlinear process systems: Handling uncertainty and unavailability of measurements," *Chem. Eng. Sci.*, vol. 63, pp. 5434–5446, 2008.