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

Fault Detection and Isolation and Safe-Parking of Networked Systems

Miao Du, Rahul Gandhi and Prashant Mhaskar

Abstract— **This work considers the problem of fault detection and isolation (FDI) and fault-handling for networked systems subject to actuator faults. The faults considered preclude the possibility of nominal operation in the affected unit. First, a model-based methodology is presented to detect and isolate faults with the explicit consideration of uncertainty. Then, an algorithm is developed to generalize the safe-parking approach for fault-tolerant control to account for complex interconnections such as parallel and recycle structures in networked systems. The efficacy of the integrated FDI and safe-parking framework is demonstrated through a chemical process example.**

I. Introduction

Faults are ubiquitous in chemical process industries and can occur in processing or control equipment such as actuators and sensors. These abnormal situations can seriously impact safety, plant economy, product quality, and pollutant emissions. To address these problems, significant research efforts have been made in the areas of fault detection and isolation (FDI) and fault-tolerant control (FTC) to devise automated methods to detect the occurrence of faults, identify the faulty unit in the control loop, and take corrective control action to prevent process performance degradation and safety hazards.

The key problem for FDI is to distinguish between the effect of "normal" disturbances to the system and a fault using various combinations of past data and first-principles based models. In the approaches using (primarily) system data, the fault information is extracted by comparing the system state trajectory with historical system data (e.g., see [1] for a review). To enhance data-based isolation for nonlinear systems, a method of decoupling the dependency between certain state variables through feedback control (exploiting the system structure) has recently been proposed (e.g., [2]). The approach using (primarily) first-principles models has been studied extensively assuming a linear system model (e.g., [3]), as well as accounting for the nonlinear nature of the system (e.g., [4], [5]).

Most of the existing results on FTC have been developed based on the assumption of the availability of sufficient residual control effort or redundant control configurations to preserve operation at the nominal equilibrium point in the presence of faults (e.g., [6], [4]). These methods can be categorized into robust/reliable control and reconfiguration-based approaches. The robust/reliable control approach (e.g., [6]) relies on the robustness of the active control configuration to handle faults as disturbances. However, some faults can hamper the available control action significantly; hence nominal operation cannot be preserved in the active control configuration regardless of the control law used. In the reconfiguration-based approach, a backup control-loop configuration is activated to preserve nominal operation with the failed control equipment disabled.

In comparison, the problem of handling faults that preclude the possibility of continued nominal operation has been paid little attention. Recently, a safe-parking framework has been proposed to handle such faults in an isolated unit in [7]. The key idea is to operate the plant at an appropriately chosen temporary equilibrium point (the so-called safe-park point) to guarantee safe operation in the presence of faults and smooth resumption of nominal operation upon fault rectification. The safe-parking framework has been extended to handle uncertainty and measurement unavailability in [8], and to handle faults for units in series in [9]. However, most processes in chemical industries use a complex integration of streams for many purposes, such as processing raw feedstock or improving the heat economy of the plant (see, e.g., [10] for control designs considering the networked nature of the system). The safe-parking mechanism for an isolated unit or units in series may not remain effective in the context of complex networked structures. Furthermore, no FDI designs are explicitly considered in [7], [8], [9].

Motivated by the above considerations, in this work we present an integrated FDI and safe-parking framework for networked systems subject to actuator faults. The faults considered preclude the possibility of nominal operation in the affected unit. The remainder of the manuscript is organized as follows. In Section II, the class of systems considered, a motivating example, and the problem statement are presented, followed by a review of the safe-parking approach. A novel FDI mechanism with the explicit consideration of uncertainty is presented in Section III. The safe-parking approach is generalized, in Section IV, to account for the complex interconnections in networked systems. In Section V, the efficacy of the integrated FDI and safe-parking framework is demonstrated through a chemical process example. Finally, Section VI presents some concluding remarks.

II. Preliminaries

In this section, we describe the class of systems considered, followed by a chemical process example, present the problem statement, and review the safe-parking approach.

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

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

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

A. System description

Consider a networked system composed of M units, described by the following ordinary differential equations:

$$
\begin{aligned}
\dot{x}_1 &= f_1(x_1) + G_1(x_1)(u_1 + \tilde{u}_1) + \sum_{j=2}^{M} R_{1,j}(x_1)x_j \\
&\quad + W_1(x_1)\theta_1 \\
&\vdots \\
\dot{x}_i &= f_i(x_i) + G_i(x_i)(u_i + \tilde{u}_i) + \sum_{j=1, j\neq i}^{M} R_{i,j}(x_i)x_j \\
&\quad + W_i(x_i)\theta_i \\
&\vdots \\
\dot{x}_M &= f_M(x_M) + G_M(x_M)(u_M + \tilde{u}_M) \\
&\quad + \sum_{j=1}^{M-1} R_{M,j}(x_M)x_j + W_M(x_M)\theta_M
\end{aligned}
\tag{1}
$$

where $x_i = [x_{i,1}, \cdots, x_{i,n_i}]^{\mathrm{T}} \in \mathbb{R}^{n_i}$, $i \in \mathcal{M} := \{1, \cdots, M\}$ denotes the vector of state variables for the ith unit, $u_i = [u_{i,1}, \cdots, u_{i,m_i}]^{\mathrm{T}} \in \mathbb{R}^{m_i}$, $i \in \mathcal{M}$ denotes the vector of constrained manipulated variables for the ith unit, taking values in a nonempty compact convex set $\mathcal{U}_i = \{u_i \in \mathbb{R}^{m_i} : u_{i,\min} \leq u_i \leq u_{i,\max}\}$, with $u_{i,\min} = [u_{i,1,\min}, \cdots, u_{i,m_i,\min}]^{\mathrm{T}}$, $u_{i,\max} = [u_{i,1,\max}, \cdots, u_{i,m_i,\max}]^{\mathrm{T}} \in \mathbb{R}^{m_i}$ the constraints on the manipulated variables, $\tilde{u}_i = [\tilde{u}_{i,1}, \cdots, \tilde{u}_{i,m_i}]^{\mathrm{T}} \in \mathbb{R}^{m_i}$ denotes the fault vector, with $u_i + \tilde{u}_i \in \mathcal{U}_i$, and $\theta_i = [\theta_{i,1}, \cdots, \theta_{i,q_i}]^{\mathrm{T}} \in \mathbb{R}^{q_i}$, $\theta_{i,\min} \leq \theta_i \leq \theta_{i,\max}$ denotes the vector of bounded (possibly time-varying) uncertain variables affecting the ith unit, with $\theta_{i,\min} = [\theta_{i,1,\min}, \cdots, \theta_{i,q_i,\min}]^{\mathrm{T}}$, $\theta_{i,\max} = [\theta_{i,1,\max}, \cdots, \theta_{i,q_i,\max}]^{\mathrm{T}} \in \mathbb{R}^{q_i}$ the bounds on uncertainty. For $i = 1, \cdots, M$, the vector function $f_i(\cdot) = [f_{i,1}(\cdot), \cdots, f_{i,n_i}(\cdot)]^{\mathrm{T}}$, where $f_{i,j}(\cdot)$ denotes the jth element of $f_i(\cdot)$, $j = 1, \cdots, n_i$, and the matrix functions $G_i(\cdot) = [g_{i,1}(\cdot)^{\mathrm{T}}, \cdots, g_{i,n_i}(\cdot)^{\mathrm{T}}]^{\mathrm{T}}$, where $g_{i,j}(\cdot)$ denotes the jth row of $G_i(\cdot)$, $j = 1, \cdots, n_i$, $R_{i,j}(\cdot) = [r_{i,j,1}(\cdot)^{\mathrm{T}}, \cdots, r_{i,j,n_i}(\cdot)^{\mathrm{T}}]^{\mathrm{T}}$, where $r_{i,j,l}(\cdot)$ denotes the lth row of $R_{i,j}(\cdot)$, $l = 1, \cdots, n_i$, and $W_i(\cdot) = [w_{i,1}(\cdot)^{\mathrm{T}}, \cdots, w_{i,n_i}(\cdot)^{\mathrm{T}}]^{\mathrm{T}}$, where $w_{i,j}(\cdot)$ denotes the jth row of $W_i(\cdot)$, $j = 1, \cdots, n_i$, are assumed to be sufficiently smooth on their domains of definition. The ith row in Eq. (1) describes the subsystem for unit i. It is assumed that the origin, i.e., $x_i = 0$, $i \in \mathcal{M}$, is an equilibrium point for each subsystem under nominal conditions (i.e., $\tilde{u}_i \equiv 0$, $\theta_i \equiv 0$, and $x_j \equiv 0$ for all $j \in \mathcal{M}\backslash\{i\}$). Each unit i is controlled by a local robust controller with a stability region denoted by $\Omega_{nom,i}$ (see [8] for one example of a robust control law with a well characterized stability region), and the state information is shared between the controllers for interconnected units. Piecewise constant control is implemented, i.e., $u(t) = u(t_k)$, for all $t \in [t_k, t_{k+1})$, where $t_k := k\Delta$, $k = 0, \cdots, \infty$, with Δ the execution period during which the control input is kept constant. It is assumed that the measurements of $x_i(t)$ for all $i \in \mathcal{M}$ are available for all $t \geq 0$.

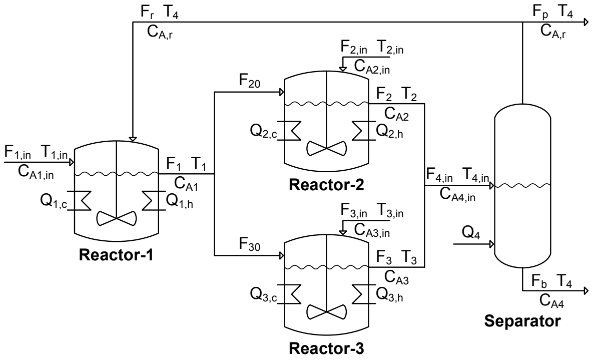

Fig. 1. Schematic of the networked process system.

B. Motivating example

To motivate the present work, we consider a networked process system comprising three reactors and a separator, as shown in Fig. 1 (a similar example is considered in [11] in the context of distributed model predictive control). In this plant, 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 in the reactors, where A is the reactant species, B the desired product, and U and R the undesired byproducts. The feed to reactor-i, $i = 1, 2, 3$, consists of reactant A at a flow rate $F_{i,in}$, concentration $C_{\mathrm{A}i,in}$, and temperature $T_{i,in}$. The outlet stream of reactor-1 at a flow rate F_1 is split into two streams such that 61.5% of the flow (F_{20}) goes to reactor-2 and the rest (F_{30}) to reactor-3. Then, the outlet streams of reactor-2 and reactor-3 go to the separator, where reactant A is separated from the products B, U, and R, and recycled back to reactor-1. It is assumed that the reactions taking place in the separator are negligible, the molecular weight of the solvent is the same as that of species A, and the products and solvent have the same volatility. Due to the nonisothermal nature of the reactions, each reactor is provided with two coils to add/remove heat to/from it. Under standard assumptions, the mathematical model for the process takes the following form:

$$
\begin{aligned}
\dot{C}_{\mathrm{A1}} &= \frac{F_{1,in}}{V_1}(C_{\mathrm{A1},in} - C_{\mathrm{A1}}) - \sum_{j=1}^{3} R_j(C_{\mathrm{A1}}, T_1) \\
&\quad + \frac{F_r}{V_1}(C_{\mathrm{A},r} - C_{\mathrm{A1}}) \\
\dot{T}_1 &= \frac{F_{1,in}}{V_1}(T_{1,in} - T_1) + \sum_{j=1}^{3} \frac{(-\Delta H_j)}{\rho c_p} R_j(C_{\mathrm{A1}}, T_1) \\
&\quad + \frac{F_r}{V_1}(T_4 - T_1) + \frac{Q_1}{\rho c_p V_1} \\
\dot{C}_{\mathrm{A2}} &= \frac{F_{2,in}}{V_2}(C_{\mathrm{A2},in} - C_{\mathrm{A2}}) - \sum_{j=1}^{3} R_j(C_{\mathrm{A2}}, T_2) \\
&\quad + \frac{F_{20}}{V_2}(C_{\mathrm{A1}} - C_{\mathrm{A2}}) \\
\dot{T}_2 &= \frac{F_{2,in}}{V_2}(T_{2,in} - T_2) + \sum_{j=1}^{3} \frac{(-\Delta H_j)}{\rho c_p} R_j(C_{\mathrm{A2}}, T_2)
\end{aligned}
$$

$$
\begin{aligned}
&+\frac{F_{20}}{V_2}(T_1-T_2)+\frac{Q_2}{\rho c_p V_2}\\
\dot{C}_{\mathrm{A3}} &= \frac{F_{3,in}}{V_3}(C_{\mathrm{A3},in}-C_{\mathrm{A3}})-\sum_{j=1}^{3}R_j(C_{\mathrm{A3}},T_3)\\
&+\frac{F_{30}}{V_3}(C_{\mathrm{A1}}-C_{\mathrm{A3}})\\
\dot{T}_3 &= \frac{F_{3,in}}{V_3}(T_{3,in}-T_3)+\sum_{j=1}^{3}\frac{(-\Delta H_j)}{\rho c_p}R_j(C_{\mathrm{A3}},T_3)\\
&+\frac{F_{30}}{V_3}(T_1-T_3)+\frac{Q_3}{\rho c_p V_3}\\
\dot{C}_{\mathrm{A4}} &= \frac{F_b}{V_4}(C_{\mathrm{A4},in}-C_{\mathrm{A4}})+\frac{F_r+F_p}{V_4}(C_{\mathrm{A4},in}-C_{\mathrm{A},r})\\
\dot{T}_4 &= \frac{F_{4,in}}{V_4}(T_{4,in}-T_4)+\frac{Q_4}{\rho c_p V_4}
\end{aligned}
$$

where $C_{\mathrm{A}i}$ is the concentration of species A, T_i is the temperature, Q_i is the rate of heat input, V_i is the volume, with subscript i denoting reactor-i (i = 1, 2, 3) or the separator (i = 4), $R_j(C_{\mathrm{A}i}, T_i) = k_{j0}e^{-E_j/RT_i}C_{\mathrm{A}i}$ is the reaction rate for the jth reaction in the ith reactor, j = 1, 2, 3, k_{j0}, E_j, and ΔH_j denote the pre-exponential constant, the activation energy, and the enthalpy of the three reactions, respectively, c_p and ρ denote the heat capacity and the density of the fluid in the reactor, respectively, and F_b, F_r, and F_p denote the flow rates of the bottom product stream, the recycle stream, and the remaining top stream from the separator, respectively. The concentration of species A in the recycle stream is computed as follows: $C_{\mathrm{A},r} = \alpha C_{\mathrm{A4}}\rho/[\rho + (\alpha - 1)C_{\mathrm{A4}}MW]$, where α is the relative volatility and MW is the molecular weight. The control objective under fault-free conditions is to operate the process at the nominal equilibrium point. The manipulated variables for reactor-i are the concentration of species A in the feed stream ($C_{\mathrm{A}i,in}$) and the rate of heat input to the reactor (Q_i). For the separator, the only manipulated variable is the rate of heat input (Q_4). It is assumed that there exist uncertainty in parameter k_{10}, sinusoidal disturbances in the inlet temperature of the feed streams, and measurement noise.

C. Problem description

Consider the networked system described by Eq. (1) with parallel and recycle structures and the failure of the mth, $m \in \{1, \cdots, m_i\}$, control actuator in unit $i \in \mathcal{M}$, which corresponds to the manipulated variable $u_{i,m}$ in Eq. (1). Let t_f and t_r denote the times that a fault takes place and it is repaired, respectively, which are unknown ahead of time. It is assumed that the failed actuator reverts to a so-called fail-safe position to prevent the occurrence of hazardous situations. Examples of fail-safe positions include shut for a heating valve and completely open for a cooling valve. Under this assumption, the output of the failed actuator (or the corresponding input of the plant under faulty conditions) is constant and known in advance, which is denoted by $\bar{u}_{i,m,f}$. The faults considered preclude the possibility of continued nominal operation in the affected unit. The problem considered in this work is as follows: 1) design of an FDI scheme with the explicit consideration of plant-model mismatch for the individual units, and 2) design of a safe-parking framework to account for the complex interconnections in networked systems.

D. Safe-parking approach for fault-tolerant control

In this section, we briefly review the safe-parking framework for an isolated unit as proposed in [7]. Let t_d denote the time that a fault is detected and isolated. Consider an isolated unit indexed by i in the networked system of Eq. (1), e.g., it is the only unit or there are no other units following it, and an actuator fault as described in Section II-C. The key idea of the safe-parking approach is to maintain the system at a suboptimal but admissible operating point (which is called a safe-park point) under faulty conditions and to resume nominal operation smoothly upon fault repair. For an isolated unit, the requirements for a safe-park point are as follows [7]: 1) the safe-park point should be a feasible equilibrium point subject to the fault, 2) it should be possible to drive the system to the safe-park point from the time t_d, i.e., the system state at the time t_d should be within the stability region of the safe-park point, which we denote by $\Omega_{s,i}$, and 3) it should be possible to resume nominal operation after the fault is rectified, i.e., the safe-park point should be within the stability region of the nominal equilibrium point. The first and third conditions require that the safe-park point be chosen from the following set:

$$
\begin{aligned}
C_i = \{x_i \in \mathbb{R}^{n_i} : f_i(x_i) + G_i(x_i)u_i = 0, u_i \in \mathcal{U}_i,\\
u_{i,m} = \bar{u}_{i,m,f}, x_i \in \Omega_{nom,i}\}
\end{aligned}
\tag{2}
$$

which is called the candidate safe-park set for unit i (subject to the stability region $\Omega_{nom,i}$).

III. Fault detection and isolation for networked systems

In this section, we design a robust FDI scheme for the individual units in the plant of Eq. (1). The key idea is to construct relations between the prescribed inputs and state measurements in the absence of faults by using the process model, while accounting for uncertainty explicitly. A fault is detected and isolated when the corresponding relation is violated. To allow fault isolation, it is assumed that there exists a state that is directly and uniquely affected by a potential fault, which is formalized in Assumption 1 below.

Assumption 1: [4] Consider the system of Eq. (1). Then for every input $u_{i,m}$, $i = 1, \cdots, M$, $m = 1, \cdots, m_i$, there exists a state $x_{i,n}$, $n \in \{1, \cdots, n_i\}$ such that with $x_{i,n}$ as an output, the relative degree of $x_{i,n}$ with respect to $u_{i,m}$ and only with respect to $u_{i,m}$ is equal to 1.

Consider the ordinary differential equation that describes the evolution of the nth state for the ith unit:

$$
\begin{aligned}
\dot{x}_{i,n} = f_{i,n}(x_i) + g_{i,n,m}(x_i)[u_{i,m}(t) + \tilde{u}_{i,m}(t)]\\
+ \sum_{j=1,j\neq i}^{M} r_{i,j,n}(x_i)x_j + w_{i,n}(x_i)\theta_i(t)
\end{aligned}
\tag{3}
$$

where $g_{i,n,m}(\cdot)$ is the mth element of the vector function $g_{i,n}(\cdot)$. As piecewise constant control is implemented, if $\tilde{u}_{i,m}(t) = 0$ for all $t \in [t_k, t_{k+1})$, we have

$$\begin{aligned}\dot{x}_{i,n} &= f_{i,n}(x_i) + g_{i,n,m}(x_i)u_{i,m}(t_k) \\ &\quad + \sum_{j=1,j\neq i}^{M} r_{i,j,n}(x_i)x_j + w_{i,n}(x_i)\theta_i(t)\end{aligned} \tag{4}$$

for $t \in [t_k, t_{k+1})$. Integrating both sides of Eq. (4) over (t_k, t_{k+1}) gives

$$\begin{aligned}x_{i,n}(t_{k+1}) &= x_{i,n}(t_k) + \int_{t_k}^{t_{k+1}} [f_{i,n}(x_i) \\ &\quad + g_{i,n,m}(x_i)u_{i,m}(t_k) \\ &\quad + \sum_{j=1,j\neq i}^{M} r_{i,j,n}(x_i)x_j + w_{i,n}(x_i)\theta_i(t)]dt\end{aligned} \tag{5}$$

Rearranging Eq. (5) yields

$$\bar{w}_{i,n}(k) = x_{i,n}(t_{k+1}) - x_{i,n}(t_k) - \bar{f}_{i,n}(k) - \bar{g}_{i,n,m}(k)u_{i,m}(t_k) \tag{6}$$

where $\bar{f}_{i,n}(k) = \int_{t_k}^{t_{k+1}} [f_{i,n}(x_i) + \sum_{j=1,j\neq i}^{M} r_{i,j,n}(x_i)x_j]dt$, $\bar{g}_{i,n,m}(k) = \int_{t_k}^{t_{k+1}} g_{i,n,m}(x_i)dt$, and $\bar{w}_{i,n}(k) = \int_{t_k}^{t_{k+1}} w_{i,n}(x_i)\theta_i(t)dt$.

Since the exact value of $\bar{w}_{i,n}(k)$ cannot be computed due to the presence of the uncertain variables, Eq. (6) cannot be directly used for FDI. However, the lower and upper bounds on $\bar{w}_{i,n}(k)$ can be computed by using the known bounds on the uncertain variables. To this end, let $\bar{w}_{i,n,l}(k)$ and $\bar{w}_{i,n,u}(k)$ denote the lower and upper bounds on $\bar{w}_{i,n}(k)$, respectively. Then, we have $\bar{w}_{i,n,l}(k) = \int_{t_k}^{t_{k+1}} w_{i,n}(x_i)\theta_{i,l}(t)dt$ and $\bar{w}_{i,n,u}(k) = \int_{t_k}^{t_{k+1}} w_{i,n}(x_i)\theta_{i,u}(t)dt$, where $\theta_{i,l}(t) = [\theta_{i,1,l}(t), \cdots, \theta_{i,q_i,l}(t)]^{\mathrm{T}}$ and $\theta_{i,u}(t) = [\theta_{i,1,u}(t), \cdots, \theta_{i,q_i,u}(t)]^{\mathrm{T}}$, with $\theta_{i,q,l}(t) = \begin{cases} \theta_{i,q,\max}, & \text{if } w_{i,n}(x_i) \leq 0 \\ \theta_{i,q,\min}, & \text{if } w_{i,n}(x_i) > 0 \end{cases}$ and $\theta_{i,q,u}(t) = \begin{cases} \theta_{i,q,\min}, & \text{if } w_{i,n}(x_i) \leq 0 \\ \theta_{i,q,\max}, & \text{if } w_{i,n}(x_i) > 0 \end{cases}$, $q = 1, \cdots, q_i$. Therefore, in the absence of the fault $\tilde{u}_{i,m}$, the following inequality holds

$$\begin{aligned}\bar{w}_{i,n,l}(k) &\leq x_{i,n}(t_{k+1}) - x_{i,n}(t_k) - \bar{f}_{i,n}(k) \\ &\quad - \bar{g}_{i,n,m}(k)u_{i,m}(t_k) \\ &\leq \bar{w}_{i,n,u}(k)\end{aligned} \tag{7}$$

Note that $\bar{g}_{i,n,m}(k) \neq 0$ because $g_{i,n,m}(\cdot) \neq 0$ under Assumption 1 and $g_{i,n,m}(\cdot)$ is continuous. This allows us to compute the lower and upper bounds on $u_{i,m}(t_k)$ from those on $\bar{w}_{i,n}(k)$. To this end, let $u_a = [x_{i,n}(t_{k+1}) - x_{i,n}(t_k) - \bar{f}_{i,n}(k) - \bar{w}_{i,n,l}(k)]/\bar{g}_{i,n,m}(k)$ and $u_b = [x_{i,n}(t_{k+1}) - x_{i,n}(t_k) - \bar{f}_{i,n}(k) - \bar{w}_{i,n,u}(k)]/\bar{g}_{i,n,m}(k)$. It follows from Eq. (7) and the physical constraints on the inputs that

$$u_{i,m,l}(k) \leq u_{i,m}(t_k) \leq u_{i,m,u}(k) \tag{8}$$

where $u_{i,m,l}(k) = \max\{u_a,\ u_{i,m,\min}\}$, $u_{i,m,u}(k) = \min\{u_b,\ u_{i,m,\max}\}$ if $\bar{g}_{i,n,m}(k) < 0$, and $u_{i,m,l}(k) = \max\{u_b,\ u_{i,m,\min}\}$, $u_{i,m,u}(t_k) = \min\{u_a,\ u_{i,m,\max}\}$ if $\bar{g}_{i,n,m}(k) > 0$. Since Eq. (8) is derived by assuming $\tilde{u}_{i,m}(t) = 0$ for all $t \in [t_k, t_{k+1})$, it follows from Eq. (3) that the only way that Eq. (8) is violated is when a fault of $\tilde{u}_{i,m}$ takes place. Therefore, if $u_{i,m}(t_k)$ breaches its lower bound $u_{i,m,l}(k)$ or upper bound $u_{i,m,u}(k)$, which can be verified through Eq. (8), then a fault associated with $u_{i,m}$ (i.e., the mth input to the ith unit) is detected and isolated simultaneously. This FDI scheme is robust in the sense that there will be no false alarms caused by uncertainty in the absence of faults. Define binary residuals as follows:

$$\text{Res}_{u_{i,j}}(k) := \begin{cases} 1, \text{ if } u_{i,j}(k) \notin [u_{i,j,l}(k), u_{i,j,u}(k)] \\ 0, \text{ otherwise} \end{cases} \tag{9}$$

A fault is declared when a non-zero residual is generated at successive n_d steps, where n_d is picked to prevent false alarms due to measurement noise.

IV. Safe-parking of networked systems with parallel and recycle structures

In this section, we propose a safe-parking framework for the networked system of Eq. (1) with parallel and recycle structures. In particular, we devise an algorithm to identify the units that need to be operated at an appropriate temporary operating point during fault rectification and generate safe-park point candidates for these units.

In the safe-parking design, we consider potential faulty scenarios with one actuator fault taking place. Let N_f denote the number of faulty scenarios under consideration and $\mathcal{N} = \{1, \cdots, N_f\}$ denote the index set for these faults. We use $\mathcal{J}_p$ to record the indices for the units that have to be safe-parked simultaneously for the pth fault, where $p \in \mathcal{N}$, which is initialized to be $\{i\}$ and updated by adding necessary entries. The determination of $\mathcal{J}_p$ is achieved by handling parallel and recycle structures alternatively. To facilitate the analysis, we consider a subsystem of Eq. (1), which is composed of K units indexed by a set $\mathcal{K} = \{i_1, \cdots, i_K\} \subseteq \mathcal{M}$ and described as follows (under nominal conditions):

$$\begin{aligned}\dot{x}_{i_1} &= f_{i_1}(x_{i_1}) + G_{i_1}(x_{i_1})u_{i_1} + \sum_{v=i_2}^{i_K} R_{i_1,v}(x_{i_1})x_v \\ &\vdots \\ \dot{x}_{i_K} &= f_{i_K}(x_{i_K}) + G_{i_K}(x_{i_K})u_{i_K} + \sum_{v=i_1}^{i_{K-1}} R_{i_K,v}(x_{i_K})x_v\end{aligned} \tag{10}$$

The above equation can be written into the following compact form:

$$\dot{x}_{\mathcal{K}} = f_{\mathcal{K}}(x_{\mathcal{K}}) + G_{\mathcal{K}}(x_{\mathcal{K}})u_{\mathcal{K}} \tag{11}$$

where $x_{\mathcal{K}} = [x_{i_1}^{\mathrm{T}}, \cdots, x_{i_K}^{\mathrm{T}}]^{\mathrm{T}} \in \mathbb{R}^{n_{\mathcal{K}}}$, with $n_{\mathcal{K}} = \sum_{v=i_1}^{i_K} n_v$, $u_{\mathcal{K}} = [u_{i_1}^{\mathrm{T}}, \cdots, u_{i_K}^{\mathrm{T}}]^{\mathrm{T}} \in \mathcal{U}_{\mathcal{K}} := \prod_{v\in\mathcal{K}} \mathcal{U}_v$, and $f_{\mathcal{K}}(\cdot)$ and $G_{\mathcal{K}}(\cdot)$ are appropriately defined.

To account for parallel structures, let $\mathcal{P}_j$ be an index set for the identified units that need to be safe-parked in the same parallel structure as unit j. We explore each unit immediately downstream of subsystem $\mathcal{P}_j$ and determine if nominal operation can be preserved by safe-parking units

$\mathcal{P}_j$. To this end, consider units indexed by $\mathcal{P}_j$ and a unit l, which is a unit immediately downstream of subsystem $\mathcal{P}_j$. To illustrate the key idea of the proposed algorithm, we assume that it has not been determined that if nominal operation can be preserved in unit l by safe-parking part of the units in $\mathcal{P}_j$ before the current exploration of unit l. We define $D_{j,l}$ as a region such that if units $\mathcal{P}_j$ operate at an equilibrium point within $D_{j,l}$, nominal operation in unit l can be preserved, which is computed as follows:

$$\begin{aligned} D_{j,l} = \{x_{\mathcal{P}_j} \in \mathbb{R}^{n_{\mathcal{P}_j}} : f_l(0) + G_l(0)u_l \\ + \sum_{v \in \mathcal{P}_j} R_{l,v}(0)x_v = 0, u_l \in \mathcal{U}_l\} \end{aligned} \quad (12)$$

Let $\mathcal{I}_j$ denote the index set for the units that are immediately downstream of those indexed by $\mathcal{P}_j$ (in the motivating example, for instance, the set $\mathcal{I}_1 = \{2, 3\}$). Let $\tilde{D}_j$ denote the intersection of $D_{j,l}$ for all $l \in \mathcal{L}_j \subseteq \mathcal{I}_j$, where $\mathcal{L}_j$ is defined as an index set for the units immediately downstream of those indexed by $\mathcal{P}_j$ in which nominal operation can be preserved.

Whenever a new $D_{j,l}$ is generated, we need to verify if there exist safe-park point candidates such that nominal operation can be preserved in unit l. We use $\mathcal{E}_p$ to record the indices of the units for which there exists at least one immediately downstream unit where nominal operation can be preserved (i.e., there exist safe-park point candidates for some units $\mathcal{P}_j$ that reside within $\tilde{D}_j$). We first compute the feasible equilibrium points subject to the reduced control action for the subsystem of Eq. (10) with $\mathcal{K} = \mathcal{J}_p$ as follows:

$$\begin{aligned} C_{\mathcal{J}_p} = \{x_{\mathcal{J}_p} \in \mathbb{R}^{n_{\mathcal{J}_p}} : f_{\mathcal{J}_p}(x_{\mathcal{J}_p}) + G_{\mathcal{J}_p}(x_{\mathcal{J}_p})u_{\mathcal{J}_p} = 0, \\ u_{\mathcal{J}_p} \in \mathcal{U}_{\mathcal{J}_p}, u_{i,m} \equiv \bar{u}_{i,m,f}, x_v \in \Omega_{nom,v} \text{ for all} \\ v \in \mathcal{J}_p, x_{\mathcal{P}_v} \in \tilde{D}_v \text{ for all } v \in \mathcal{E}_p\} \end{aligned} \quad (13)$$

The component equilibrium points are chosen as safe-park point candidates for subsystem $\mathcal{P}_j$, which are denoted by set C_j. If $C_j \cap D_{j,l} \neq \varnothing$, then there exist safe-park point candidates such that nominal operation can be preserved in unit l. For this case, we add $\mathcal{P}_j$ to $\mathcal{E}_p$ and l to $\mathcal{L}_j$. If $C_j \cap D_{j,l} = \varnothing$, we need to safe-park unit l as well and therefore add l to $\mathcal{J}_p$. For the units where nominal operation cannot be preserved, we further explore the downstream units for each of them by following the above procedure.

If a recycle structure is encountered as the exploration proceeds, it may not be true that nominal operation can still be preserved in units $\mathcal{L}_v$ (the set determined by following the procedure for parallel structures) for all $v \in \mathcal{E}_p$. To solve this problem, we treat units $\mathcal{J}_p$ as a subsystem and examine (or reexamine) if nominal operation can be preserved in each unit downstream of this subsystem by following the method developed for parallel structures to maximize the possibility of nominal operation in individual units. The exploration terminates when nominal operation can be preserved in all the downstream units of the subsystem $\mathcal{J}_p$ or this subsystem has no downstream units.

After the units that need to be safe-parked are identified, a bank of safe-park point candidates for the subsystem $\mathcal{J}_p$ can be generated according to Eq. (13). In contrast to [9], we choose the component equilibrium points of those in $C_{\mathcal{J}_p}$ for each unit as the safe-park point candidates for the individual units. The stability region of the safe-park point candidate for each unit is then computed by using the steady-state values of the states of the upstream units and treating the deviations of their actual values from the steady-state values as disturbances. The off-line design of the safe-parking framework for the networked system of Eq. (1) is formalized in Algorithm 1 below.

Algorithm 1: This algorithm describes the off-line design of the safe-parking framework for the networked system of Eq. (1).

1) Design a local controller for each unit, indexed by $j \in \mathcal{M}$, and characterize the stability region of the corresponding nominal equilibrium point, denoted by $\Omega_{nom,j}$. Let $\mathcal{Q} = \mathcal{N}$.
2) Pick p from $\mathcal{Q}$ and remove p from $\mathcal{Q}$. Let $\mathcal{S} = \mathcal{J}_p = \{i\}$ and $\mathcal{E}_p = \varnothing$.
    a) If $\mathcal{S} \neq \varnothing$, pick $j \in \mathcal{S}$ and remove $\mathcal{P}_j$ from $\mathcal{S}$, else go to Step 3.
    b) If no recycle structure is detected, let $\mathcal{T} = \mathcal{I}_j \backslash \mathcal{J}_p$, else let $\mathcal{L}_v = \varnothing$ for all $v \in \mathcal{E}_p$, $\mathcal{E}_p = \varnothing$, $\mathcal{S} = \{v \in \mathcal{J}_p : \mathcal{I}_v \backslash \mathcal{J}_p \neq \varnothing\}$, and go to Step 2a.
    c) If $\mathcal{T} \neq \varnothing$, characterize $D_{j,l}$ for units $\mathcal{P}_j$ and some $l \in \mathcal{T}$, as defined in Eq. (12), and remove l from $\mathcal{T}$, else go to Step 2a.
    d) If $C_j \cap D_{j,l} \neq \varnothing$, add $\mathcal{P}_j$ to $\mathcal{E}_p$ and l to $\mathcal{L}_j$ (initialized as $\varnothing$), else add l to $\mathcal{S}$ and $\mathcal{J}_p$. Go to Step 2c.
3) Generate safe-park point candidates $x_{s,j}$ for each unit $j \in \mathcal{J}_p$ according to Eq. (13).
4) Characterize the stability regions, denoted by $\Omega_{s,j}$, for all the safe-park point candidates $x_{s,j}$.
5) If $\mathcal{Q} \neq \varnothing$, repeat Step 2.

Upon FDI, we search over the results of the off-line design to choose safe-park points for the units which have to be operated at a temporary operating point during fault rectification (i.e., units indexed by $\mathcal{J}_p$ if the pth fault takes place). We stabilize these units at safe-park points, while stabilizing the remaining units at nominal equilibrium points.

Remark 1: The proposed algorithm provides a systematic procedure to confine the effect of the fault in a subsystem of the networked plant. While we focus on the occurrence of one actuator fault in the safe-parking design, this methodology can be generalized to handle multiple faults (possibly in different units in the context of a networked plant) by considering the combination of fail-safe positions for most commonly encountered faulty scenarios in practice.

V. Simulation Example

Consider the networked process example of Section II-B. The Lyapunov-based robust model predictive controller of [8] is designed for each unit by using a quadratic Lyapunov function of the form $V_i = x_i^{\mathrm{T}} P_i x_i$. The control execution period is chosen as $\Delta = 0.025$ hr $= 1.5$ min and a two-step prediction horizon is used. The noisy measurements are

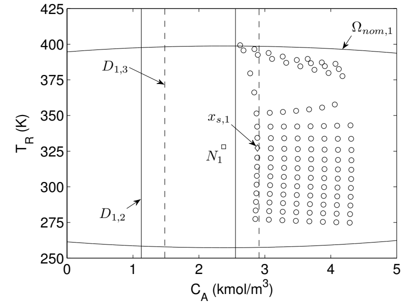

Fig. 2. Stability region of the nominal equilibrium point for reactor-1 ($\Omega_{nom,1}$), sets $D_{1,2}$ and $D_{1,3}$, and feasible equilibrium points (marked by circles and the diamond) subject to the fault in $C_{A1,in}$ for reactor-1 in the subsystem.

filtered before performing FDI and computing the prescribed input.

Consider a fault in $C_{A1,in}$, for which we implement Algorithm 1 (some details are omitted). To account for the recycle stream, we plot the temporary equilibrium points for reactor-1 by using the model for the subsystem composed of reactor-1, reactor-2, and the separator, as shown in Fig. 2. Since there exist feasible equilibrium points within $D_{1,3}$ (e.g., $x_{s,1}$ in Fig. 2), nominal operation can be preserved in reactor-3. Therefore, we have $\mathcal{J} = \{1, 2, 4\}$, $\mathcal{E} = \{1\}$, and $\mathcal{L} = \{3\}$. It means that reactor-1, reactor-2, and the separator have to be safe-parked simultaneously, with nominal operation in reactor-3 preserved. The process operates at the nominal equilibrium point initially. The fault is introduced at time $t_f = 1$ hr and repaired at time $t_r = 2.5$ hr. As shown in Fig. 3, the proposed FDI scheme detects and isolates the fault very quickly at time $t = 1.025$ hr and the fault is confirmed at time $t_d = 1.125$ hr, with $n_d = 5$. Subsequently, reactor-1, reactor-2, and the separator are safe-parked, with reactor-3 continuing nominal operation even during fault rectification and the entire plant resuming nominal operation upon fault rectification. The evolution of the closed-loop state profiles are depicted in Fig. 4.

VI. Conclusions

This work considered the problem of FDI and fault-handling for networked systems subject to actuator faults. The faults considered preclude the possibility of nominal operation in the affected unit. First, a model-based methodology was presented to detect and isolate faults with the explicit consideration of uncertainty. Then, an algorithm was developed to generalize the safe-parking approach for fault-tolerant control to account for complex interconnections such as parallel and recycle structures in networked systems. The efficacy of the integrated FDI and safe-parking framework was demonstrated through a chemical process example.

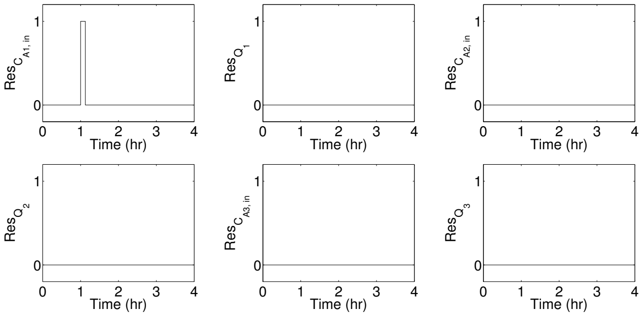

Fig. 3. Residuals for the manipulated variables $C_{Ai,in}$ and Q_i for the three reactors, i = 1, 2, 3. The fault in $C_{A1,in}$ is first detected and isolated at time $t = 1.025$ hr and then confirmed at $t_d = 1.125$ hr.

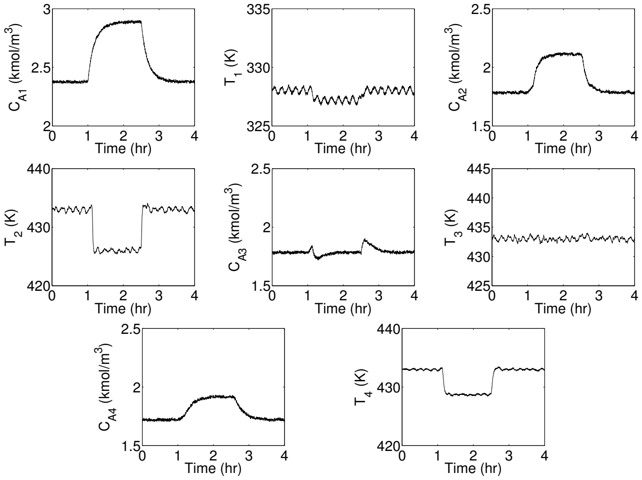

Fig. 4. Evolution of the closed-loop state profiles for reactor-1, reactor-2, reactor-3, and the separator, where simultaneous safe-parking is implemented for reactor-1, reactor-2, and the separator.

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] B. J. Ohran, D. Muñoz de la Peña, J. F. Davis, and P. D. Christofides, "Enhancing data-based fault isolation through nonlinear control," *AIChE J.*, vol. 54, pp. 223–241, 2008.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9] R. Gandhi and P. Mhaskar, "A safe-parking framework for plant-wide fault-tolerant control," *Chem. Eng. Sci.*, vol. 64, pp. 3060–3071, 2009.

[10] E. Tatara, I. Birol, F. Teymour, and A. Cinar, "Agent-based control of autocatalytic replicators in networks of reactors," *Comp. & Chem. Eng.*, vol. 29, pp. 807–815, 2005.

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