2011 50th IEEE Conference on Decision and Control and
European Control Conference (CDC-ECC)
Orlando, FL, USA, December 12-15, 2011

Control, Monitoring and Reconfiguration of Sampled-Data Hybrid Process Systems with Actuator Faults

Ye Hu and Nael H. El-Farra[†]
Department of Chemical Engineering & Materials Science
University of California, Davis, CA 95616 USA

Abstract— **This work presents an integrated model-based framework for control, fault detection and control system reconfiguration of hybrid process systems with measurement sampling rate constraints and actuator faults. A family of output feedback controllers are initially synthesized to stabilize each fault-free subsystem with the aid of a dynamic inter-sample model predictor for each mode. The stability properties for each closed-loop subsystem are then analyzed to obtain the maximum allowable sampling period together with an explicit characterization of the fault-free behavior of each mode. Conditions that guarantee asymptotic stability of the overall switched system are also derived and used to examine the interplay between the selection of the sampling period, the model, the controller and observer design parameters, and the dwell time for each mode. To detect actuator faults within a given mode, a time-varying alarm threshold based on the fault-free behavior is obtained and used, and when faults are detected, actuator reconfiguration is performed to maintain closed-loop stability. A key idea of the reconfiguration strategy is to take into account not only the stability properties of the current mode, but also the stabilizing ability and availability of the fall-back actuator configurations for the future modes. The design and implementation of the developed methodology are demonstrated using a hybrid chemical reactor example.**

I. Introduction

With the extensive use of automated control systems in modern chemical plants, a great deal of emphasis is being placed on process safety and reliability issues because of the increased likelihood of faults, such as malfunctions of process equipment and/or control instrumentation, which can undermine the stability and integrity of the entire system if not detected and handled appropriately. Not surprisingly, the problems of fault detection and fault-tolerant control of dynamic process systems have been the subject of considerable research interest over the past few decades in both the academic and industrial circles in process control (e.g., see [1]–[9] and the references therein). A careful examination of the existing literature on process monitoring, however, shows that the majority of existing methods have been developed for purely continuous processes. Yet, many chemical processes are characterized by strong interactions between continuous dynamics and discrete events, and are more appropriately modeled as hybrid systems. Compared with the efforts on the analysis and control of hybrid systems (e.g., see [10] for some results and references in this area), the monitoring and reconfiguration problems have received less attention. Examples of important contributions on monitoring of hybrid systems include the design of switched state estimation schemes for switched linear systems [11]–[13], and the development of fault diagnosis algorithms using hybrid automata theory [14], hybrid bond graph models [15], [16], and statistical data-based methods [17].

Recently, we developed in [18] an integrated approach for fault detection and monitoring of a class of hybrid process systems modeled by switched nonlinear systems with control actuator faults, uncertain continuous dynamics and uncertain mode transitions. A robust hybrid monitoring scheme that distinguishes reliably between faults, mode transitions and uncertainty was developed using tools from unknown input observer theory and results from Lyapunov stability theory.

Beyond uncertainty and hybrid dynamics, measurement sampling is another key issue that requires attention in the design of the monitoring and control systems. In practice, measurements of the process outputs are typically available from the sensors at discrete time instants with the transmission frequency dictated by the inherent limitations on the data collection and processing capabilities of the sensors or the communication medium. Due to these limitations, the design and implementation of the monitoring and control system are further complicated in that the ability of the system to accurately monitor the evolution of the process and implement correct, yet prompt, control actions will be impaired by discrete measurement sampling, and this might lead to performance deterioration or even loss of stability.

Motivated by these considerations, we present in this work a methodology for control, fault detection and control system reconfiguration for hybrid process systems subject to measurement sampling constraints and actuator faults. To compensate for measurement unavailability, a model of each mode of the hybrid system is embedded within the corresponding output feedback controller to provide estimates of the output measurements between sampling instants. The output of the model is then updated and reset using the actual measurements whenever they become available from the sensors. An augmented system is then formulated and its stability properties are studied, which leads to an explicit characterization, for each mode, of the fault-free behavior and the maximum allowable sampling period that ensures the global exponential stability of each sampled-data closed-loop subsystem. Furthermore, since the stability of every subsystem doesn't necessarily imply the stability of the overall

[†] To whom correspondence should be addressed: E-mail: nhelfarra@ucdavis.edu.

978-1-61284-799-3/11/$26.00 ©2011 IEEE

switched system when there are an infinite number of mode transitions, additional requirements on the control system design that are sufficient to guarantee the asymptotic stability of the entire system are proposed. To detect actuator faults within the constituent modes, we utilize the characterized fault-free behavior of each subsystem to derive the actuator fault detection rules. And based on the stabilizing ability and availability of the fall-back actuator configurations, the control system reconfiguration logic is proposed that ensures the stability of the current mode as well as the future modes.

The rest of the paper is organized as follows. In Section II, we describe the mathematical model for the class of systems considered in this work. A family of output feedback controllers are then designed in Section III, followed by the analysis of the stability properties of the sampled-data closed-loop subsystem and the overall switched system. The fault detection scheme is presented next in Section IV, together with the switching logic of the fall-back actuator configurations in the event of faults. Finally, the proposed theoretical framework is illustrated in Section V using a hybrid chemical process example.

II. Preliminaries

We consider the class of switched systems represented by the following state-space description:

$$\begin{aligned} &\dot{x}(t) = A_{i(t)}x(t) + B_{i(t)}(u_{i(t)}(t) + f_{i(t)}(t)),\ t \in [t^{\text{in}}_{i^k}, t^{\text{out}}_{i^k}) \\ &y(t) = Cx(t),\ i(t) \in \mathcal{I} = \{1, 2, \cdots, N\},\ k \in \mathbb{N} \end{aligned} \tag{1}$$

where $x \in \mathbb{R}^n$ denotes the vector of continuous-time state variables, $u_i \in \mathbb{R}^m$ denotes the vector of manipulated input variables for the i-th mode (or subsystem), $f_i \in \mathbb{R}^m$ denotes the control actuator fault in the i-th mode, $y \in \mathbb{R}^p$ denotes the vector of output variables. A_i, B_i, and C are $n \times n$, $n \times m$, and $p \times n$ matrices, respectively. The switching signal $i(t) : \mathbb{R}^+ \to \mathcal{I}$ is assumed to be a piecewise continuous (from the right) function of time, which implies that there are only a finite number of switches during a finite interval of time, and it represents a discrete-valued state that indexes A_i, B_i, $u_i(\cdot)$ and $f_i(\cdot)$, which altogether determine the evolution of x when the i-th mode is active. It is assumed that x does not exhibit discontinuous jumps when the mode transitions take place, which means that x is everywhere continuous. The notations $t^{\text{in}}_{i^k}$ and $t^{\text{out}}_{i^k}$ are used to represent the k-th time that the i-th mode is switched in and out, respectively. In this work, we consider the case where the switching schedule is fixed (i.e., both the times and the sequence of the mode transitions are pre-determined) and the dwell time $T_{i^k} \triangleq t^{\text{out}}_{i^k} - t^{\text{in}}_{i^k}$ is an integer multiple of the sampling period h_{i^k} for all $i \in \mathcal{I}$ and $k \in \mathbb{N}$, i.e., $T_{i^k} = \mathcal{N}_{i^k} h_{i^k}$ where $\mathcal{N}_{i^k} \in \mathbb{N}$. In addition, we assume that the entrance time of each mode $t^{\text{in}}_{i^k}$ is also the initial sampling instant of that period.

III. Controller synthesis and stability analysis in the absence of faults

In this section, we discuss the synthesis of an output feedback controller for each fault-free constituent subsystem, and then we shall characterize the stability properties and obtain the maximum allowable sampling period for each sampled-data closed-loop subsystem, and finally the stability properties of the overall switched system are investigated.

A. Output feedback controller synthesis

In sampled-data systems, measurements of the output are available only at discrete time instants. One way to handle this constraint in the context of control of hybrid systems is to embed a dynamic model of each mode within the corresponding controller to provide it with an estimate of the output between sampling instants, and to reset the model estimate using the output when it becomes available to correct possible estimation errors. To this end, we consider, for each mode, a dynamic model of the following form:

$$\begin{aligned} &\dot{\bar{x}} = \bar{A}_i\bar{x} + \bar{B}_iu_i,\ \ i \in \mathcal{I} \\ &\bar{y}(t) = C\bar{x}(t),\ t \in (t^j_{i^k}, t^{j+1}_{i^k});\ \bar{y}(t) = y(t),\ t = t^j_{i^k} \end{aligned} \tag{2}$$

where $\bar{x} \in \mathbb{R}^n$ and $\bar{y} \in \mathbb{R}^p$ denote the estimates of x and y, u_i denotes the control input, $\bar{A}_i$ and $\bar{B}_i$ are constant matrices that model A_i and B_i, $t^j_{i^k}$ denotes the time of the j-th update during the period that the i-th mode is active for the k-th time where $j \in \mathbb{N}$. At sampling instants, $\bar{y}$ is reset by the actual output y; however, unless C has a two-sided inverse or a left inverse, the model state $\bar{x}$ cannot be uniquely determined from $\bar{y}$, and thus the evolution of $\bar{x}$ cannot be corrected by the update performed on $\bar{y}$. To circumvent this problem, we propose the following procedure that allows constructing a new model for each mode based on (2):

1) Define $y_{\text{m}} = \bar{C}x$, $\ \bar{y}_{\text{m}} = \bar{C}\bar{x}$, where $y_{\text{m}} \in \mathbb{R}^r$ denotes the vector of measurements that are not redundant (we shall hereafter use "trimmed output" to refer to y_{m}), $\bar{y}_{\text{m}}$ denotes an estimate of y_{m}, $\bar{C}$ is an $r \times n$ matrix that contains all the linearly independent rows in C (in the same order), where $r \triangleq \text{rank}(C)$.
2) Obtain the reduced row echelon form of C using elementary row operations and then identify all the non-basic variables of $\bar{x}$, which are used to form a new column vector $\bar{x}_{\text{um}} \in \mathbb{R}^{n-r}$ which we shall refer to as the estimate of the unmeasured state.
3) Define $\widehat{x} = [\bar{y}'_{\text{m}}\ \bar{x}'_{\text{um}}]' = [\bar{C}'\ \bar{E}']'\bar{x} = \widehat{P}\bar{x}$ where, for each row of $\bar{E}$, the entry whose location corresponds to the index of the associated non-basic variable in $\bar{x}$ is 1 and all the remaining entries are 0. Note that $\widehat{P}$ is invertible by construction.

Based on this procedure, the new model can be introduced:

$$\begin{aligned} \dot{\widehat{x}} &= \begin{bmatrix} \dot{\bar{y}}_{\text{m}} \\ \dot{\bar{x}}_{\text{um}} \end{bmatrix} = \begin{bmatrix} \widehat{A}^{11}_i & \widehat{A}^{12}_i \\ \widehat{A}^{21}_i & \widehat{A}^{22}_i \end{bmatrix} \begin{bmatrix} \bar{y}_{\text{m}} \\ \bar{x}_{\text{um}} \end{bmatrix} + \begin{bmatrix} \widehat{B}^{11}_i \\ \widehat{B}^{21}_i \end{bmatrix} u_i \\ &= \widehat{A}_i\widehat{x} + \widehat{B}_iu_i,\ \ \ i \in \mathcal{I} \\ \widehat{y}(t) &= \bar{y}_{\text{m}}(t) = \widehat{C}\widehat{x}(t),\ \ \ t \in (t^j_{i^k}, t^{j+1}_{i^k}) \\ \widehat{y}(t) &= \bar{y}_{\text{m}}(t) = y_{\text{m}}(t),\ \ \ t = t^j_{i^k},\ \ \ j, k \in \mathbb{N} \end{aligned} \tag{3}$$

with $\widehat{x} \in \mathbb{R}^n$ and $\widehat{y} \in \mathbb{R}^r$ denoting respectively the model state and model output, $\widehat{A}_i = \widehat{P}\bar{A}_i\widehat{P}^{-1}$, $\widehat{B}_i = \widehat{P}\bar{B}_i$, $\widehat{C} = [I_{r\times r}\ O_{r\times n-r}]$. Notice that updating the model output using the actual measurements at each sampling instant influences the evolution of $\widehat{x}$ since the model output is part of the model state. Based on this inter-sample model predictor, we consider the following output feedback controller design:

$$\begin{aligned} &\dot{\chi}(t) = \widehat{A}_i\chi(t) + \widehat{B}_iu_i(t) + L_i(\widehat{y}(t) - \widehat{C}\chi(t)) \\ &\eta(t) = \widehat{P}^{-1}\chi(t),\ \ u_i(t) = K_i\eta(t) \end{aligned} \tag{4}$$

where $\chi \in \mathbb{R}^n$ is the observer state which is an estimate of $\widehat{x}$, $\eta \in \mathbb{R}^n$ is the observer output which is an estimate of

$\bar{x}$, K_i is the feedback gain, and L_i is the observer gain that should be chosen to ensure that $\widehat{A}_i - L_i\widehat{C}$ is Hurwitz for all i which requires that $(\widehat{A}_i, \widehat{C})$ be a detectable pair.

B. Stability of the sampled-data closed-loop subsystems

To explicitly characterize the maximum allowable sampling period for each closed-loop subsystem, we first define the model estimation error as $e = \widehat{y} - y_{\text{m}}$ where $e \in \mathbb{R}^r$ represents the difference between the model output and the trimmed output, and the augmented state vector as $\xi = [x' \ \chi' \ \bar{x}'_{\text{um}} \ e']' \in \mathbb{R}^{3n}$. Then the augmented system that governs the evolution of ξ can be formulated as follows:

$$\begin{aligned} \dot{\xi}(t) &= \Lambda_i \xi(t), \quad t \in (t_{i^k}^{j}, t_{i^k}^{j+1}) \\ \xi(t) &= I_s \xi(t^-), \quad t = t_{i^k}^{j}, \quad i \in \mathcal{I}, \quad j,k \in \mathbb{N} \end{aligned} \tag{5}$$

where $\Lambda_i =$

$$\begin{bmatrix} A_i & B_i K_i \widehat{P}^{-1} & O_{n\times n-r} & O_{n\times r} \\ L_i \bar{C} & \widehat{A}_i + \widehat{B}_i K_i \widehat{P}^{-1} - L_i \widehat{C} & O_{n\times n-r} & L_i \\ \widehat{A}_i^{21} \bar{C} & \widehat{B}_i^{21} K_i \widehat{P}^{-1} & \widehat{A}_i^{22} & \widehat{A}_i^{21} \\ \widehat{A}_i^{11}\bar{C} - \bar{C}A_i & (\widehat{B}_i^{11} - \bar{C}B_i)K_i\widehat{P}^{-1} & \widehat{A}_i^{12} & \widehat{A}_i^{11} \end{bmatrix}$$

and $I_s = \begin{bmatrix} I_{n\times n} & O_{n\times n} & O_{n\times n-r} & O_{n\times r} \\ O_{n\times n} & I_{n\times n} & O_{n\times n-r} & O_{n\times r} \\ O_{n-r\times n} & O_{n-r\times n} & I_{n-r\times n-r} & O_{n-r\times r} \\ O_{r\times n} & O_{r\times n} & O_{r\times n-r} & O_{r\times r} \end{bmatrix}$.

It's worth noting that, in the augmented state ξ, the process state x, the observer state χ and the estimate of the unmeasured state $\bar{x}_{\text{um}}$ all evolve continuously over time, while the model estimation error e gets reset to zero at each sampling instant. Therefore, we can obtain the closed-loop response of (5) as follows (see [19] for a similar proof):

$$\xi(t) = e^{\Lambda_i (t - t_{i^k}^{j})} (I_s e^{\Lambda_i h_{i^k}})^{j-1} \xi(t_{i^k}^{\text{in}}), \quad t \in [t_{i^k}^{j}, t_{i^k}^{j+1}) \tag{6}$$

where $\xi(t_{i^k}^{\text{in}}) = [x'(t_{i^k}^{\text{in}}) \ \chi'(t_{i^k}^{\text{in}}) \ \bar{x}'_{\text{um}}(t_{i^k}^{\text{in}}) \ O_{1\times r}]'$, $h_{i^k} \triangleq t_{i^k}^{j+1} - t_{i^k}^{j}$. It can be seen from (6) that the stability of the origin of the augmented system is dictated by the matrix $M_i \triangleq I_s e^{\Lambda_i h_{i^k}}$ as both $e^{\Lambda_i (t - t_{i^k}^{j})}$ and $\xi(t_{i^k}^{\text{in}})$ are bounded, and thus the necessary and sufficient condition for the origin to be globally exponentially stable is that all the eigenvalues of the matrix M_i should lie inside the unit circle, in which case we can obtain the following bound on the size of the augmented state ξ (a proof can be found in [19]):

$$\|\xi(t)\| \le \alpha_{i^k} \|\xi(t_{i^k}^{\text{in}})\| e^{-\beta_{i^k}(t - t_{i^k}^{\text{in}})}, \quad t \in [t_{i^k}^{\text{in}}, t_{i^k}^{\text{out}}) \tag{7}$$

where we use $\|\cdot\|$ to denote the Euclidean norm for a vector or a matrix, $\alpha_{i^k} \ge 1$ and $\beta_{i^k} > 0$ are some constants.

Remark 1. By examining the expression of the matrix M_i, it can be seen that it is dependent on the sampling period h_{i^k} as well as the matrix Λ_i which in turn depends on the model matrices, the feedback gain K_i and the observer gain L_i. All these parameters represent degrees of freedom that can be adjusted to ensure that all the eigenvalues of M_i are strictly inside the unit circle. Furthermore, for a given set of design parameters for the model, controller and observer, the maximum allowable sampling period for a given mode $h_i^{\max}$ can be determined by evaluating the spectral radius of M_i as a function of h_{i^k}. Any choice of the sampling period h_{i^k} that satisfies $h_{i^k} \in (0, h_i^{\max})$ guarantees stability of the i-th sampled-data closed-loop subsystem.

Remark 2. In general, different subsystems have different maximum allowable sampling periods. In practice, to ensure stability of the origin for each closed-loop subsystem, one can switch the sampling period when a mode transition takes place so that the new sampling period is stabilizing for the active mode, or to use a common sampling period that is stabilizing for all the modes. However, the latter may result in unnecessarily frequent sampling for certain modes.

C. Stability of the overall switched system

For switched systems that involve an infinite number of mode transitions on the infinite time interval, stability of all the subsystems is not sufficient to guarantee stability of the overall switched system. Here we use the tool of multiple Lyapunov functions (MLF) to analyze the stability of the overall switched system of (5) and derive conditions that ensure stability. To this end, converse Lyapunov theorems for discontinuous dynamical systems (see Theorem 9 in [20]) can be used to show that, for each exponentially stable subsystem of (5), there exists a function $V_i : \mathbb{R}^{3n} \to \mathbb{R}^+$ that satisfies the following inequalities for all $\xi(t) \in \mathbb{R}^{3n}$ where $t \in [t_{i^k}^{\text{in}}, t_{i^k}^{\text{out}})$:

$$a_i \|\xi(t)\|^{d_i} \le V_i(\xi(t)) \le b_i \|\xi(t)\|^{d_i} \tag{8a}$$

$$V_i(\xi(t)) \le \psi_i\big(V_i(\xi(t_{i^k}^{j}))\big), \quad t \in [t_{i^k}^{j}, t_{i^k}^{j+1}) \tag{8b}$$

$$DV_i(\xi(t_{i^k}^{j})) \le -c_{i^k} V_i(\xi(t_{i^k}^{j})) \tag{8c}$$

where a_i, b_i, c_{i^k} and d_i are some positive constants, $\psi_i(\cdot) : \mathbb{R}^+ \to \mathbb{R}^+$ is a continuous function that satisfies $\psi_i(0) = 0$ and $\lim_{\theta\to 0}[\psi_i(\theta)/\theta^q] = 0$ for some $q > 0$, and

$$DV_i(\xi(t_{i^k}^{j})) \triangleq [V_i(\xi(t_{i^k}^{j+1})) - V_i(\xi(t_{i^k}^{j}))]/h_{i^k}$$

The explicit form of $\psi_i(\cdot)$ can be obtained by using (8a) for $t \in [t_{i^k}^{j}, t_{i^k}^{j+1})$ as follows:

$$\begin{aligned} V_i(\xi(t)) &\le b_i \|\xi(t)\|^{d_i} \le b_i \left(\|\xi(t_{i^k}^{j})\| \|e^{\Lambda_i (t - t_{i^k}^{j})}\| \right)^{d_i} \\ &\le \frac{b_i \widetilde{\alpha}_{i^k}}{a_i} a_i \|\xi(t_{i^k}^{j})\|^{d_i} \le \frac{b_i \widetilde{\alpha}_{i^k}}{a_i} V_i(\xi(t_{i^k}^{j})) \end{aligned} \tag{9}$$

where $\widetilde{\alpha}_{i^k} \triangleq e^{\sigma_{\max}(\Lambda_i) h_{i^k} d_i}$ with $\sigma_{\max}(\cdot)$ denoting the largest singular value of a matrix; and, thus, $\psi_i(\theta) = b_i \widetilde{\alpha}_{i^k} \theta / a_i$, which shows that $\psi_i(\cdot)$ is a class $\mathcal{K}$ function.

A sufficient condition for the overall switched system to be globally asymptotically stable (e.g., [21], [22]) is to have:

$$V_i(\xi(t_{i^{k+1}}^{\text{out}-})) < V_i(\xi(t_{i^k}^{\text{out}-})), \quad \forall i \in \mathcal{I}, \quad \forall k \in \mathbb{N} \tag{10}$$

which requires that, for any given $i \in \mathcal{I}$, $V_i(\xi(t_{i^k}^{\text{out}-}))$ be decreasing for $k \in \mathbb{N}$. The following theorem provides an explicit condition that characterizes how the sampling period, the model, and the controller/observer design parameters, should be chosen to ensure satisfaction of (10) and global asymptotic stability of the overall switched system of (5).

Theorem 1. *Consider the switched system of* (5)*, where, for all $i \in \mathcal{I}$, the model parameters $\widehat{A}_i$ and $\widehat{B}_i$, the feedback gain K_i and the observer gain L_i are chosen such that all the eigenvalues of the matrix M_i are strictly inside the unit circle. Then if the following inequality is also satisfied for all $i \in \mathcal{I}$ and all $k \in \mathbb{N}$:*

$$\frac{\left(\Xi(t_{i^{k+1}}^{\text{in}}) \|\xi(0)\| e^{-\Phi(t_{i^{k+1}}^{\text{in}})} \right)^{d_i}}{\left\| [\chi'(t_{i^k}^{\text{out}-}) \ \ \bar{x}'_{\text{um}}(t_{i^k}^{\text{out}-})]' \right\|^{d_i}} < \frac{a_i^2}{b_i^2 \widetilde{\alpha}_{i^k} (1 - h_{i^{k+1}} c_{i^{k+1}})^{\mathcal{N}_{i^{k+1}} - 1}} \tag{11}$$

where

$$\Xi(t^{\text{in}}_{i^{k+1}}) \triangleq \prod_{i=1}^{N} \prod_{k=1}^{\kappa_i(t^{\text{in}}_{i^{k+1}})} \alpha_{i^k},\ \Phi(t^{\text{in}}_{i^{k+1}}) \triangleq \sum_{i=1}^{N} \sum_{k=1}^{\kappa_i(t^{\text{in}}_{i^{k+1}})} \beta_{i^k} T_i$$

where $\kappa_i(t)$ denotes the number of times that the i-th mode has been activated by time t (the modes that have never been active are not qualified for the above summation and multiplication calculations), the origin of the overall switched system of (5) *is globally asymptotically stable.*

Proof. For the overall switched system of (5) to be globally asymptotically stable, (10) must always be satisfied. However, at $t = t^{\text{in}}_{i^{k+1}}$, the value of $V_i(\xi(t^{\text{out}-}_{i^{k+1}}))$ is not known but it can be estimated using the current information and (8b)-(8c). To this end, by rearranging (8c) we can obtain:

$$V_i(\xi(t^{j+1}_{i^{k+1}})) \leq (1 - h_{i^{k+1}} c_{i^{k+1}}) V_i(\xi(t^{j}_{i^{k+1}}))$$

which, together with $t^{\text{out}}_{i^{k+1}} - t^{\text{in}}_{i^{k+1}} = \mathcal{N}_{i^{k+1}} h_{i^{k+1}}$, leads to:

$$\begin{aligned} V_i(\xi(t^{\mathcal{N}_{i^{k+1}}}_{i^{k+1}})) &\leq (1 - h_{i^{k+1}} c_{i^{k+1}}) V_i(\xi(t^{\mathcal{N}_{i^{k+1}}-1}_{i^{k+1}})) \\ &\leq \cdots \leq (1 - h_{i^{k+1}} c_{i^{k+1}})^{\mathcal{N}_{i^{k+1}}-1} V_i(\xi(t^{\text{in}}_{i^{k+1}})) \end{aligned}$$

Applying (8b) for $t \in (t^{\mathcal{N}_{i^{k+1}}}_{i^{k+1}}, t^{\text{out}}_{i^{k+1}})$ and using the properties of class $\mathcal{K}$ function yields:

$$V_i(\xi(t^{\text{out}-}_{i^{k+1}})) \leq \psi_i\left((1 - h_{i^{k+1}} c_{i^{k+1}})^{\mathcal{N}_{i^{k+1}}-1} V_i(\xi(t^{\text{in}}_{i^{k+1}}))\right)$$

Thus, to ensure that (10) is always satisfied, we must have:

$$\psi_i\left((1 - h_{i^{k+1}} c_{i^{k+1}})^{\mathcal{N}_{i^{k+1}}-1} V_i(\xi(t^{\text{in}}_{i^{k+1}}))\right) < V_i(\xi(t^{\text{out}-}_{i^k})) \tag{12}$$

For the right-hand side of (12), since $\xi(t)$ contains $x(t)$ which is not available, we can use $\big\|[\chi'(t) \quad \bar{x}'_{\text{um}}(t)]'\big\| \leq \|\xi(t)\|$, together with (8a), to conclude that

$$a_i \Big\|[\chi'(t^{\text{out}-}_{i^k}) \quad \bar{x}'_{\text{um}}(t^{\text{out}-}_{i^k})]'\Big\|^{d_i} \leq V_i(\xi(t^{\text{out}-}_{i^k}))$$

where both χ and $\bar{x}_{\text{um}}$ are known for all times. For the left-hand side of (12), since the model estimation error e is the only component in ξ that does not evolve continuously and is reset to zero at each sampling instant, we have $\|\xi(t^{\text{in}}_{i^{k+1}})\| \leq \|\xi(t^{\text{in}-}_{i^{k+1}})\|$. Suppose the previous active mode is mode ϵ in its l-th activation period, then, we can do this calculation in a chain using (7) until we reach the initial time at $t = 0$:

$$\begin{aligned} \|\xi(t^{\text{in}}_{i,k+1})\| &\leq \|\xi(t^{\text{in}-}_{i,k+1})\| = \|\xi(t^{\text{out}-}_{j,l})\| \\ &\leq \alpha_{j,l}\|\xi(t^{\text{in}}_{j,l})\| e^{-\beta_{j,l}T_j} \leq \alpha_{j,l}\|\xi(t^{\text{in}-}_{j,l})\| e^{-\beta_{j,l}T_j} \\ &\leq \cdots \leq \Xi(t^{\text{in}}_{i,k+1})\|\xi(0)\| e^{-\Phi(t^{\text{in}}_{i,k+1})} \end{aligned} \tag{13}$$

Since $\psi_i(\cdot)$ belongs to class $\mathcal{K}$, by using (8a), we have:

$$\begin{aligned} &\psi_i\big((1 - h_{i^{k+1}} c_{i^{k+1}})^{\mathcal{N}_{i^{k+1}}-1} b_i(\Xi(t^{\text{in}}_{i^{k+1}})\|\xi(0)\| e^{-\Phi(t^{\text{in}}_{i^{k+1}})})^{d_i}\big) \\ &\qquad \geq \psi_i\big((1 - h_{i^{k+1}} c_{i^{k+1}})^{\mathcal{N}_{i^{k+1}}-1} V_i(\xi(t^{\text{in}}_{i^{k+1}}))\big) \end{aligned}$$

Therefore, if

$$\begin{aligned} &\psi_i\big((1 - h_{i^{k+1}} c_{i^{k+1}})^{\mathcal{N}_{i^{k+1}}-1} b_i(\Xi(t^{\text{in}}_{i^{k+1}})\|\xi(0)\| e^{-\Phi(t^{\text{in}}_{i^{k+1}})})^{d_i}\big) \\ &\qquad < a_i \Big\|[\chi'(t^{\text{out}-}_{i^k}) \quad \bar{x}'_{\text{um}}(t^{\text{out}-}_{i^k})]'\Big\|^{d_i} \end{aligned} \tag{14}$$

then (12) will always be satisfied which implies the satisfaction of (10), and thus the overall switched system of (5) will be globally asymptotically stable. Rearrangement of (14) using (9) yields (11) which completes the proof. □

Remark 3. Since (8c) describes only the constraint on the values of the Lyapunov function at the sampling instants when the model estimation error is reset to zero, this inequality essentially specifies a decay rate for the other three components in ξ (i.e., x, χ and $\bar{x}_{\text{um}}$) between the sampling instants, and thus c_{i^k} is in general dependent on the model, the controller and observer design parameters. As for $\widetilde{\alpha}_{i^k}$, it can be seen from its definition that it is also dependent on the aforementioned parameters as well as the sampling period. Therefore, when switching into a new mode, (11) should be checked, and, if not satisfied, one or more of the available degrees of freedom (the sampling period, the model, the controller and the observer parameters) should be adjusted to ensure satisfaction of the stability condition. For example, if the model, the feedback and observer gains are fixed, the sampling period can be adjusted within the range $(0, h^{\max}_i)$ to ensure stability. However, if (11) cannot be satisfied for any of the allowable values of the design parameters, a modification of the switching schedule by prolonging the dwell time for the current mode becomes necessary.

IV. Observer-based fault detection and control system reconfiguration

In this section, we describe how the fault-free behavior of the augmented system obtained in the previous section can be used as the basis for deriving rules for the detection of actuator faults within each constituent mode. We also discuss the reconfiguration of the control system in the event of faults so that the stability of the process can be preserved.

A. Fault detection within the constituent modes

It can be shown that, when the sampling period of each mode is less than its maximum allowable value, $h^{\max}_i$, and there are no faults, i.e., $f_i(t) \equiv 0$, the observer output η is expected to satisfy the following bound for $t \in [t^{\text{in}}_{i^k}, t^{\text{out}}_{i^k})$:

$$\|\eta(t)\| \leq \|\widehat{P}^{-1}\|\|\xi(t)\| \leq \bar{\alpha}_{i^k}\|\xi(t^{\text{in}}_{i^k})\| e^{-\beta_{i^k}(t - t^{\text{in}}_{i^k})} \tag{15}$$

where $\bar{\alpha}_{i^k} \triangleq \|\widehat{P}^{-1}\|\alpha_{i^k}$. This bound can be used as the basis for deriving rules for actuator fault detection. Specifically, for any given mode i in its k-th time of activation, when there is no actuator fault, the evolution of η satisfies (15); conversely, if $\|\eta(t)\| > \bar{\alpha}_{i^k}\|\xi(t^{\text{in}}_{i^k})\| e^{-\beta_{i^k}(t - t^{\text{in}}_{i^k})}$, then we know that an actuator fault has occurred in mode i. However, the information $\|\xi(t^{\text{in}}_{i^k})\|$ is not accessible due to the unavailability of x. So, the calculations in (13) are used to estimate $\|\xi(t^{\text{in}}_{i^k})\|$, and an actuator fault is detected at time t_{d} if

$$\|\eta(t_{\text{d}})\| > \bar{\alpha}_{i^k}\Xi(t^{\text{in}}_{i^k})\|\xi(0)\| e^{-\Phi(t^{\text{in}}_{i^k})T_i} e^{-\beta_{i^k}(t_{\text{d}} - t^{\text{in}}_{i^k})} \tag{16}$$

Remark 4. By proper tuning of the controller and observer design parameters, $\bar{\alpha}_{i^k}$ and β_{i^k} in (16) can be made sufficiently tight to ensure that the actuator fault detection delay is minimized. It should also be noted that this stability-based fault detection scheme can be used to detect both incipient and abrupt actuator faults, simultaneous faults, and faults that appear in process equipment and measurement sensors, as long as the stability properties are altered by the faults.

B. Control system reconfiguration

Immediately after an actuator fault is detected, the control system should be reconfigured to avert performance degradation or instability. In this work, reconfiguration is performed by activating a fall-back actuator configuration. It is assumed that none of the actuator configurations have identical back-ups, and that all the modes operate with a common sampling period that is smaller than the maximum allowable sampling periods (associated with the initial actuator configuration) for all the modes. However, when the system switches to a different mode, the sampling period can be reduced for the duration of the new mode if (11) is not satisfied.

The control system reconfiguration for hybrid systems differs from that for continuous systems in the sense that the activation of a fall-back actuator configuration for continuous systems defines a different mode, while for hybrid systems, that defines a "sub-mode" within the active mode. For example, for mode i at its k-th time of activation, if an actuator breaks down and a new actuator configuration is deployed, the input matrix B_i changes and thus a new "sub-mode" within mode i is created, which has a new maximum allowable sampling period $\bar{h}_i^{\max}$ for the given model, controller and observer design parameters, and a new fault detection alarm threshold. To stabilize the current operating mode using the sampling period h_{i^k} that has been chosen at the beginning of this period , $\bar{h}_i^{\max}$ must be larger than h_{i^k}. Also, if no more faults take place in the future, the newly activated actuator configuration will continue to be used in the subsequent operating modes. For each of these future modes, there will also be a maximum allowable sampling period associated with this actuator configuration, which we denote by $\bar{h}_\pi^{\max}$ for $\pi \in \mathcal{I} - \{i\}$. Then, if for any of the future modes, $\bar{h}_\pi^{\max} \leq h$, stability of that mode will be lost. This suggests that stability properties of the future modes should be considered when activating a certain fall-back actuator configuration within a given mode.

Another complication rests in the fact that the actuator configuration that is selected may not be available for all modes. If such an actuator configuration is still functional when an operating mode that does not have it becomes active, stability will be compromised. Based on the above analysis, we summarize the actuator reconfiguration logic as follows:

1) Calculate the maximum allowable sampling periods for all the possible combinations of operating modes and their corresponding actuator configurations.
2) When an actuator fault takes place, choose the fall-back actuator configurations that are available for all future operating modes and whose corresponding maximum allowable sampling periods $\bar{h}_i^{\max}$ are greater than h for all the modes that will become active.

Remark 5. For switched systems with only a finite number of mode transitions, the MLF criterion need not be considered and so the appropriate operating sampling periods for all the modes and "sub-modes" can be calculated prior to process operation. However, if there are an infinite number of mode switches, the MLF criterion should be considered every time the system enters a mode (by verifying (11)) or a "sub-mode" (by verifying a slightly modified version of (11)) and the sampling period may have to be adjusted if necessary.

V. Simulation study: application to a chemical reactor with multiple operating modes

To illustrate the implementation of the methodology proposed in this work, we consider a continuous stirred tank reactor (CSTR) where an irreversible first-order elementary exothermic reaction of the form $A \xrightarrow{k_0} B$ takes place. The reactor has three operating modes: for mode 1, the reactor has one inlet stream providing fresh A at flow rate F_1, molar concentration C_{A1} and temperature T_{A1}; for mode 2, another stream containing A at flow rate F_2, molar concentration C_{A2} and temperature T_{A2} is added; for mode 3, a third stream feeding A at flow rate F_3, molar concentration C_{A3} and temperature T_{A3} is introduced. The mode transitions are triggered by changes in operating requirements and a jacket is used to provide or remove heat due to the non-isothermal nature of the reaction. The mathematical model for this process takes the following form:

$$\dot{C}_A = \sum_{\iota=1}^{3} \sigma_\iota(t) \frac{F_\iota}{V}(C_{A\iota} - C_A) - k_0 \exp\left(\frac{-E}{RT}\right) C_A$$

$$\dot{T} = \sum_{\iota=1}^{3} \sigma_\iota(t) \frac{F_\iota}{V}(T_{A\iota} - T) - \frac{\Delta H_r}{\rho c_p} k_0 \exp\left(\frac{-E}{RT}\right) C_A + \frac{Q}{\rho c_p V}$$

where C_A denotes the concentration of A, T denotes the reactor temperature, ι is the feed stream index, $\sigma_\iota(t)$ can be either 0 or 1, representing the removal or addition of a new feed stream, V is the reactor volume, k_0, E, ΔH_r are the pre-exponential constant, the activation energy, and the enthalpy of the reaction, R is the gas constant, c_p and ρ denote the heat capacity and density of the fluid in the reactor, Q is the rate of heat input to the reactor. For different operating modes, the reactor has different actuator configurations (for simplicity, it is assumed that each configuration has only one manipulated input): for mode 1, Q, C_{A1} and T_{A1} can be used; for mode 2, C_{A2} and T_{A2} are also available; for mode 3, C_{A3} and T_{A3} can be used as well. Using typical values for the process parameters, the reactor with the manipulated inputs at their respective nominal values usually has three equilibrium points for each mode: two locally asymptotically stable and one unstable. Our control objective is to stabilize the temperature at 375 K. The corresponding unstable equilibrium points for the three modes are $[C_A^{1s}\ T^s]' = [3.75\,\text{mol/L}\ 375\,\text{K}]'$, $[C_A^{2s}\ T^s]' = [4.00\,\text{mol/L}\,375\,\text{K}]'$, $[C_A^{3s}\,T^s]' = [4.25\,\text{mol/L}\,375\,\text{K}]'$, respectively. In the simulations, we assume that measurements of T are available. Defining the displacement variables $x = [x_1\ x_2]' = [C_A - C_A^{1s}\ T - T^s]'$ places the equilibrium point for the first mode x_1^s at the origin, and the equilibrium points for the second and third modes at $x_2^s = [0.25\,\text{mol/L}\,0\,\text{K}]'$ and $x_3^s = [0.50\,\text{mol/L}\,0\,\text{K}]'$. And then the linearized model of the reactor is obtained using standard linearization techniques.

TABLE I

Maximum allowable sampling periods (hour) for operating mode-actuator configuration combinations

	Q	C_{A1}	T_{A1}	C_{A2}	T_{A2}	C_{A3}	T_{A3}
Mode 1	0.41	0.39	0.41	N/A	N/A	N/A	N/A
Mode 2	0.55	0.71	0.55	0.71	0.55	N/A	N/A
Mode 3	1.03	1.22	1.03	1.22	1.03	1.22	1.03

Following the methodology presented in Section III, a dynamic model is constructed (the explicit form is omitted here for brevity) and an output feedback controller is designed for each mode based on the linearized system. The feedback and observer gains are chosen such that the poles of $\widehat{A}_i + \widehat{B}_i K_i \widehat{P}^{-1}$ are placed at $(-5,\ -10)$ and the poles of $\widehat{A}_i - L_i \widehat{C}$ are at $(-20,\ -50)$. With the model, controller and observer design parameters fixed, the maximum allowable sampling periods for all the combinations of operating modes and actuator configurations are computed (see Table I). This table will be used as the basis for selecting the fall-back actuator configurations in the event of faults.

In the following closed-loop simulations, the actuator configuration Q is initially used and the sampling period is chosen to be $0.4\,\text{hr}$ which is smaller than the maximum allowable sampling periods associated with Q for all the modes (see Table I). The reactor is initialized in mode 1, and the switching sequence is given by: mode 1 $\xrightarrow{@25\,\text{hr}}$ mode 2 $\xrightarrow{@50\,\text{hr}}$ mode 3. Based on the methodology presented in Section IV-A, the fault-free behavior of the observer output for each mode is used as the basis for fault detection. As can be seen from Fig. 1(a), shortly after the beginning of operation, the reactor temperature has already been successfully stabilized at the steady-state value as well as the reactant concentration. At $t = 5\,\text{hr}$, a malfunction is introduced in the cooling jacket, and the norm of the observer output $\|\eta\|$ breaches the alarm threshold (see Fig. 1(b)) which demands that a new actuator configuration be activated to preserve stability. Since the sampling period for all the modes is fixed at $0.4\,\text{hr}$, we can conclude from Table I that only T_{A1} can be used as the fall-back actuator configuration because it is available for both modes 2 and 3, and its maximum allowable sampling periods for all the modes are greater than $0.4\,\text{hr}$. Since the activation of T_{A1} actuator configuration introduces a "sub-mode" within mode 1, a new fault detection alarm threshold is used. At $t = 25\,\text{hr}$, a mode transition takes place, and $0.33\,\text{hr}$ after that, a fault is detected and a fall-back actuator configuration must be activated again. This time, all the available actuator configurations can be used since their maximum allowable sampling periods are all greater than $0.4\,\text{hr}$. T_{A2} is chosen here which results in a new fault detection threshold. Two hours later, it becomes faulty since $\|\eta\|$ breaches the fault detection threshold, and the cooling jacket (we assume that it has been repaired by this time) is used again until it breaks down at $t = 55\,\text{hr}$ when the reactor is already in mode 3. At this time, C_{A3} is activated and used as the manipulated input for all future times.

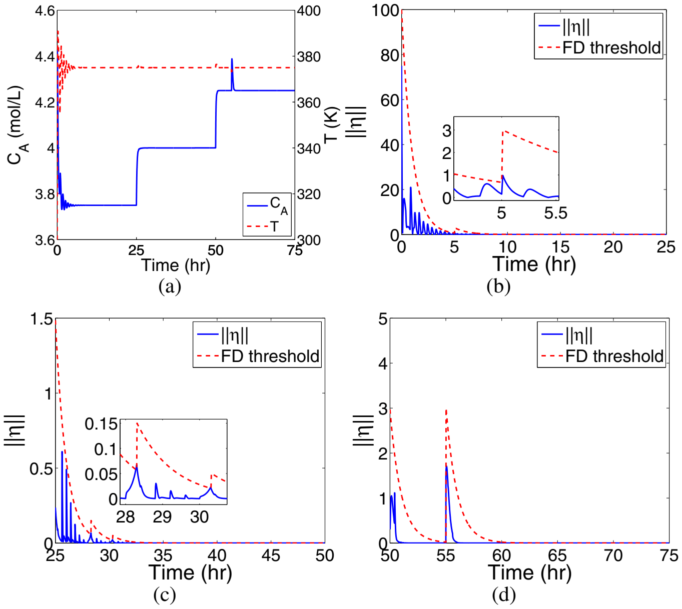

Fig. 1. Evolution of the closed-loop state (1(a)) and the norm of the observer output (1(b)-1(d)) under mode transitions and actuator faults.

References

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

[2] M. Basila, G. Stefanek, and A. Cinar, "A model-object based supervisory expert system for fault tolerant chemical reactor control," *Comput. Chem. Eng.*, vol. 14, pp. 551–560, 1990.

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

[4] B. Huang, "Bayesian methods for control loop monitoring and diagnosis," *J. Process Control*, vol. 18, no. 9, pp. 829 – 838, 2008.

[5] 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.

[6] A. Armaou and M. Demetriou, "Robust detection and accommodation of incipient component faults in nonlinear distributed processes,," *AIChE J.*, vol. 54, pp. 2651–2662, 2008.

[7] S. Ghantasala and N. H. El-Farra, "Robust actuator fault isolation and management in constrained uncertain parabolic PDE systems," *Automatica*, vol. 45, pp. 2368–2373, 2009.

[8] S. Perk, F. Teymour, and A. Cinar, "Statistical monitoring of complex chemical processes using agent-based systems," *Ind. Eng. Chem. Res*, vol. 49, no. 11, pp. 5080–5093, 2010.

[9] M. Mahmood and P. Mhaskar, "Safe-parking framework for fault-tolerant control of transport-reaction processes," *Ind. Eng. Chem. Res*, vol. 49, no. 9, pp. 4285–4296, 2010.

[10] P. D. Christofides and N. H. El-Farra, *Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-Delays.* Berlin/Heidelberg: Springer-Verlag, 2005.

[11] A. Balluchi, L. Benvenuti, M. D. Di Benedetto, and A. L. Sangiovanni-Vincentelli, "Design of observers for hybrid systems," in *Hybrid Systems: Computation and Control.* Berlin/Heidelberg: Springer-Verlag, 2002, pp. 76–89.

[12] W. Wang, D. H. Zhou, and Z. Li, "Robust state estimation and fault diagnosis for uncertain hybrid systems," *Nonlinear Anal. Theory Methods Appl.*, vol. 65, pp. 2193–2215, 2006.

[13] A. Alessandri, M. Baglietto, and G. Battistelli, "Luenberger observers for switching discrete-time linear systems," *Int. J. Control*, vol. 80, pp. 1931–1943, 2007.

[14] F. Zhao, X. Koutsoukos, H. Haussecker, J. Reich, and P. Cheung, "Monitoring and fault diagnosis of hybrid systems," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 35, pp. 1225–1240, 2005.

[15] M. Basseville, A. Benveniste, and L. Tromp, "Diagnosing hybrid dynamical systems: Fault graphs, statistical residuals and viterbi algorithms," in *Proc. 37th IEEE Conf. on Decision and Control*, Tampa, FL, 1998, pp. 3757–3762.

[16] S. Narasimhan and G. Biswas, "Model-based diagnosis of hybrid systems," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 37, pp. 348–361, 2007.

[17] X. Jin and B. Huang, "Robust identification of piecewise/switching autoregressive exogenous process," *AIChE J.*, vol. 56, no. 7, pp. 1829–1844, 2010.

[18] Y. Hu and N. H. El-Farra, "Robust fault detection and monitoring of hybrid process systems with uncertain mode transitions," *AIChE J.*, in press.

[19] L. A. Montestruque and P. J. Antsaklis, "On the model-based control of networked systems," *Automatica*, vol. 39, pp. 1837–1843, 2003.

[20] A. Michel, "Recent trends in the stability analysis of hybrid dynamical systems," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 46, no. 1, pp. 120 –134, Jan. 1999.

[21] M. S. Branicky, "Multiple Lyapunov functions and other analysis tools for switched and hybrid systems," *IEEE Trans. Autom. Control*, vol. 43, pp. 475–482, 1998.

[22] H. Ye, A. N. Michel, and L. Hou, "Stability theory for hybrid dynamical systems," *IEEE Trans. Autom. Control*, vol. 43, pp. 461–474, 1998.