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

Robust Fault Detection and Reconfigurable Control of Distributed Energy Generation Systems

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

Abstract— **This paper focuses on robust model-based fault detection and fault-tolerant control of distributed energy generation systems subject to time-varying external disturbances and control actuator faults. An observer-based output feedback controller that enforces robust stability with an arbitrary degree of disturbance attenuation in the absence of faults is initially designed for each subsystem. Fault detection is performed locally by comparing the output of the observer with that of the system, and using the discrepancy as a residual. An explicit characterization of the fault-free behavior of the closed-loop system is obtained in terms of a time-varying bound that captures the effects of discrete measurement sampling, plant-model mismatch, and external disturbances. This characterization is used to derive a time-varying alarm threshold on the residual for robust fault detection, and a controller reconfiguration law that determines the feasible fall-back control configurations that preserve robust stability and minimize performance deterioration. Contingency measures in the event that local fault recovery is not possible are discussed. Finally, the design and implementation of the integrated monitoring and fault-tolerant control architecture are demonstrated using a simulated model of a solid oxide fuel cell plant.**

I. Introduction

Distributed power generation refers to the integrated or stand-alone use of small, modular electric generation deployed close to the point of consumption. Examples of distributed power sources include internal combustion engines coupled with generators, micro-turbines, fuel cells, and renewable systems such as photovoltaic arrays and wind turbines. Such distributed resources offer advantages over conventional grid electricity by offering end users a diversified fuel supply; higher power reliability, quality, and efficiency; lower emissions and greater flexibility to respond to changing energy needs [1], [2]. However, a distributed power network with a large number of small generators requires far more sophisticated monitoring and control systems than a radial grid focused on a few big plants. This has motivated significant research work over the past decade on the development and implementation of control strategies for various kinds of distributed energy generation systems (e.g., see [3], [4], [5], [6], [7], [8], [9], [10], [11] for some results and references in this area).

Compared with the significant and growing body of research work on control of distributed energy systems, the problem of integrating fault detection and handling capabilities in the control system design has received less attention. The significance of this problem stems from the fact that the distributed power market is primarily driven by the need for high-quality power and the fact that the impact of local faults in the distributed power network can be quite substantial, especially when the power sources are grid-connected and the disruptions in power supply caused by local failures has the potential to cascade through the network and interfere with grid operations. An effort to address this problem was initiated in [12] where a model-based framework for the detection and compensation of faults was developed. The basic idea was to integrate fault detection and control system reconfiguration at the local level with higher-level supervisory control measures in the event that local fault rectification was not possible.

In addition to the need for fault detection, one of the key issues that needs to be accounted for in the design of any model-based fault-tolerant control system is robustness with respect to time-varying exogenous disturbances which typically arise during the operation of power generation systems. Such disturbances, if not properly accounted and compensated for, can degrade the stability and performance properties of the individual systems, and can also interfere with the fault diagnosis and fault recovery processes leading to false or missed alarms and poor supervisory control. These considerations provide a strong incentive for the development of robust monitoring and fault-tolerant control systems that enable distributed generation systems to provide highly reliable services under disturbances and fault scenarios.

To address this problem, we present in this paper a methodology for the integrated design of robust fault detection and reconfigurable control systems for distributed energy systems subject to external disturbances and control actuator faults. The rest of the paper is organized as follows. Following some preliminaries and an overview of the problem formulation in Section II, a solid-oxide fuel cell plant model is presented in Section III as a motivating example. An observer-based robust output feedback controller design that enforces closed-loop stability and disturbance attenuation in the absence of faults is then presented and analyzed in Section IV. An explicit characterization of the fault-free behavior of the closed-loop system is obtained in terms of a time-varying bound that captures the combined effects of measurement sampling, plant-model mismatch, and external

† To whom correspondence should be addressed: E-mail: nhelfarra@ucdavis.edu. Financial support by the UC Energy Institute is gratefully acknowledged.

disturbances. The results are then used in Section V to derive the necessary rules for robust fault detection and recovery through control system reconfiguration. Both stability and performance considerations are addressed in the design of the fault-tolerant control system, and supervisory control measures in the event that local fault recovery is not possible are discussed. Numerical simulations are presented in each section to demonstrate the implementation of the various components of the fault-tolerant control architecture.

II. Preliminaries and problem formulation

We consider a collection of distributed energy generation resources managed by a higher-level supervisor. Each resource is modeled by a continuous-time system with the following state–space description:

$$\begin{array}{rcl} \dot{x}_i & = & f_i(x_i) + G_i^{k(t)}(x_i)[u_i^{k(t)} + f_{a,i}^{k(t)}] + W_i(x_i)d_i(t) \\ y_i & = & h_i(x_i, u_i), \;\; k(t) \in \mathcal{K}_i := \{1, \cdots, N_i\} \end{array} \quad (1)$$

where $x_i \in \mathbb{R}^{n_i}$ denotes the vector of state variables associated with the i–th subsystem (e.g., exhaust temperatures and rotation speed in turbines and internal combustion engines, operating temperature and pressure in fuel cells), $y_i \in \mathbb{R}^{q_i}$ is the vector of measured and/or controlled outputs (e.g., output power, temperature, voltage and frequency), $d_i \in \mathbb{R}^{r_i}$ is the vector of time-varying (but bounded) external disturbance inputs, $u_i^k \in \mathbb{R}^{m_i}$ denotes the vector of manipulated inputs associated with the k-th control configuration in the i–th subsystem (e.g., inlet fuel and air flow rates in fuel cells, shaft speed in turbines), $f_{a,i}^k$ is a fault in the control actuators of the k-th control configuration, $k(t)$ is a discrete variable that specifies which control configuration is active at time t, N_i is the number of available control configurations for the i–th subsystem, and $f_i(\cdot)$, $G_i^k(\cdot)$, $W_i(\cdot)$ and $h_i(\cdot)$, are sufficiently smooth nonlinear functions. In general, the perturbation term is considered to be non-vanishing, i.e., the nominal and perturbed systems do not share the same equilibrium point.

Referring to the system of Eq.1, the control objective is to robustly stabilize each subsystem around the desired set-point in the presence of control actuator faults and external disturbances using sampled measurements of the output at discrete times. To ensure fault-tolerance, a number of different control configurations are assumed to be available. Only one of these configurations is used for control at any given time while the rest are kept dormant for possible use as backup in the event of faults. The problems under consideration include how to regulate the states of each subsystem in the absence of faults and suppress the influences of external disturbances using discretely-sampled measurements, how to detect faults in the operating control configuration in the presence of disturbances in a timely fashion, and how to reconfigure the local control system to maintain the desired stability and performance properties.

III. Motivating example: Temperature control in a solid oxide fuel cell

To illustrate the design and implementation of the robust fault-tolerant control system to be presented in this work, we consider a solid oxide fuel cell (SOFC) plant as an example (see the plant model in [10]). Fuel cells are important distributed resources due to their high efficiency, low levels of environmental pollution, and flexible modular designs that match versatile demands of customers. The control objective is to regulate the temperature of the fuel cell stack around a desired set-point in the presence of time-varying disturbances in the load current. The set-point is assumed to be determined by the supervisor based on its knowledge of the load changes in the distributed power network that it manages. Measurements of the SOFC stack temperature are collected at discrete sampling times and sent to the local controller where the control action is calculated and sent back to the actuator. Three control configurations are considered: one uses the inlet fuel flow rate as the manipulated input (configuration 1), while the other two employ, respectively, the inlet air flow rate (configuration 2) and the temperature of the feed (configuration 3) as the manipulated variable.

To simplify the controller design and implementation, we consider the problem on the basis of the linearization of the fuel cell plant model around the desired set-point:

$$\dot{x} = Ax + B^k[u^k + f_a^k] + Ed, \;\; y = Cx, \;\; k = 1, 2, 3 \quad (2)$$

where x, u^k, d and y are the state, manipulated input, disturbance input and measured output vectors for the plant, respectively, defined by $x = [\frac{x_{H_2} - x_{H_2}^s}{x_{H_2}^s} \;\; \frac{x_{O_2} - x_{O_2}^s}{x_{O_2}^s} \;\; \frac{x_{H_2O} - x_{H_2O}^s}{x_{H_2O}^s} \;\; \frac{T_s - T_s^s}{T_s^s}]^T$, $u^1 = \frac{q_{H_2}^{in} - q_{H_2}^{in,s}}{q_{H_2}^{in,s}}$, $u^2 = \frac{q_{O_2}^{in} - q_{O_2}^{in,s}}{q_{O_2}^{in,s}}$, $u^3 = \frac{T_{in} - T_{in,s}}{T_{in,s}}$, $d = \frac{I - I^s}{I^s}$, $y = \frac{T_s - T_s^s}{T_s^s}$ where, $i : H_2, \; O_2, \; H_2O$, x_i and q_i^{in} are respectively the mole fraction and inlet molar flow rate of component i, T_s is the stack temperature, T_{in} is the temperature of the feed, the superscript s denotes the steady state values of the corresponding states and inputs, and A, B^k, E, and C are constant matrices given by:

$$A = \begin{bmatrix} -0.0350 & 0 & 0 & 0 \\ 0 & -0.3139 & 0 & 0 \\ 0 & 0 & -0.0117 & 0 \\ -0.0031 & -0.0077 & -0.0008 & -0.0110 \end{bmatrix},$$

$B^1 = [0.0437 \;\; 0 \;\; 0 \;\; 0.0027]^T$, $B^2 = [0 \;\; 0.3304 \;\; 0 \;\; 0.0063]^T$, $B^3 = [0 \;\; 0 \;\; 0 \;\; 0.0130]^T$, $E = [-0.0087 \;\; -0.0164 \;\; 0.0117 \;\; 0.0038]^T$ and $C = [0 \; 0 \; 0 \; 1]$.

In the next two sections, we describe how the control strategy is tailored to take the disturbances and faults explicitly into account. We begin in Section IV with the design and analysis of the robust fault-free control system. The results serve as the basis for tackling the robust fault detection and control system reconfiguration problems in Section V.

IV. Robust fault-free control: synthesis, analysis and implementation

The objective of this section is to design for each actuator configuration an output feedback controller that enforces (in the absence of faults) robust closed-loop stability using sampled measurements, and to characterize the minimum allowable sampling rate necessary to guarantee practical

closed-loop stability with an arbitrary degree of attenuation of the effect of disturbances on the closed-loop state.

A. Robust output feedback controller synthesis

We consider an output feedback controller of the form:

$$u^k = F^k\eta, \;\; \dot{\eta} = \widehat{A}\eta + \widehat{B}^k u^k + L(y - C\eta) \tag{3}$$

where F^k is the feedback gain, η is the state of an observer that generates estimates of x using y, $\widehat{A}$ and $\widehat{B}^k$ are constant matrices that represent models of A and B^k, respectively, and L is the observer gain. Note that in general $\widehat{A} \neq A$ and $\widehat{B}^k \neq B^k$ to allow for possible plant-model mismatch. The feedback and observer gains are chosen to account for the effect of the disturbances and to enforce practical closed-loop stability in the absence of discrete sampling. Specifically, given any positive real numbers, D and r, the controller and observer gains are chosen such that if $\|d(t)\| \leq D$ for all $t \geq 0$, the closed-loop state norm is ultimately bounded by r, i.e., $\limsup_{t\to\infty}\|x(t)\| \leq r$, where r can be made arbitrarily small by appropriate selection of F^k and L. This argument can be justified using standard Lyapunov techniques and is omitted for brevity.

To address the problem when the output measurements are not available continuously, we include within the local control system a dynamic model of the plant of Eq.2 to provide the observer with an estimate of the measured output when measurements are not available from the sensors. The state of the model is then updated using the actual output measurements whenever they are provided by the sensors at sampling times. Specifically, we consider an inter-sample model predictor of the form:

$$\begin{aligned} \dot{w}_1 &= \widehat{A}_{11}w_1 + \widehat{A}_{12}w_2 + \widehat{B}_1^k u^k \\ \dot{w}_2 &= \widehat{A}_{21}w_1 + \widehat{A}_{22}w_2 + \widehat{B}_2^k u^k \end{aligned} \tag{4}$$

where $w_1 = \widehat{y}$ is an estimate of the plant output (e.g., the SOFC stack temperature), and w_2 is the vector of the remaining model states (which provide estimates of the unmeasured plant states), $\widehat{A} = \begin{bmatrix} \widehat{A}_{11} & \widehat{A}_{12} \\ \widehat{A}_{21} & \widehat{A}_{22} \end{bmatrix}$, $\widehat{B}^k = [\widehat{B}_1^{k^T} \quad \widehat{B}_2^{k^T}]^T$. With the aid of this inter-sample model predictor, the output feedback controller can be implemented as follows:

$$\begin{aligned} u^k(t) &= F^k\eta(t), \;\; t \in (t_j, t_{j+1}) \\ \dot{\eta}(t) &= \widehat{A}\eta(t) + \widehat{B}^k u^k(t) + L(\widehat{y}(t) - C\eta(t)) \\ \dot{w}_1(t) &= \widehat{A}_{11}w_1(t) + \widehat{A}_{12}w_2(t) + \widehat{B}_1^k u^k(t), \widehat{y}(t) = w_1(t) \\ \dot{w}_2(t) &= \widehat{A}_{21}w_1(t) + \widehat{A}_{22}w_2(t) + \widehat{B}_2^k u^k(t) \\ \widehat{y}(t_j) &= y(t_j), \; j = 0, 1, 2, \cdots \end{aligned} \tag{5}$$

where t_j is the j-th sampling instance and $\Delta := t_{j+1} - t_j$ is the sampling period. Note that only the output of the model is re-set using the actual output at the sampling times. Note also that a choice of $\widehat{A}_{11} = O$, $\widehat{A}_{12} = O$, $\widehat{B}_1^k = O$, corresponds to the special case of sample-and-hold where in between consecutive sampling times the last available measurement is held until the next one is available.

B. Robust closed-loop stability analysis

To simplify the analysis, we focus on the typical case where the sampling period is constant (extensions to the case of time-varying sampling periods are possible and the subject of other research work). To characterize the maximum allowable sampling period (equivalently, the minimum sampling rate) between the sensors and the controller, we define the model estimation error as $e(t) = w_1(t) - y(t) = w_1(t) - Cx(t)$, where $e \in \mathbb{R}^q$ represents the difference between the output of the model and the output of the plant. Defining the augmented state vector $\chi = \begin{bmatrix} x^T & \eta^T & w_2^T & e^T \end{bmatrix}^T$, it can be shown that the augmented system can be formulated as a combined discrete-continuous system of the form:

$$\begin{aligned} \dot{\chi}(t) &= \Lambda_o^k\chi(t) + Hd(t), \;\; t \in (t_j, t_{j+1}) \\ e(t_j) &= 0, \;\; j = 0, 1, 2, \cdots; \; t_{j+1} - t_j = \Delta \end{aligned} \tag{6}$$

where

$$\Lambda_o^k = \begin{bmatrix} A & B^kF^k & O & O \\ LC & \widehat{A} + \widehat{B}^kF^k - LC & O & L \\ \widehat{A}_{21}C & \widehat{B}_2^kF^k & \widehat{A}_{22} & \widehat{A}_{21} \\ \widehat{A}_{11}C - CA & \widehat{B}_1^kF^k - CB^kF^k & \widehat{A}_{12} & \widehat{A}_{11} \end{bmatrix} \tag{7}$$

is a constant matrix and $H = [E^T \; O \; O \; -(CE)^T]^T$. Note that while the plant state, the observer state, and the estimate of the unmeasured states all evolve continuously over time, the error is re-set to zero at each transmission instance since the output of the model is updated every Δ seconds using the true output measurement.

The following proposition provides an explicit characterization of the sampled-data closed-loop system behavior in the absence of faults. The proof can be obtained by solving Eqs.6-7 and using induction, and will be omitted for brevity.

Proposition 1: The system described by Eqs.6-7 with initial condition $\chi(t_0) = \begin{bmatrix} x^T(t_0) & \eta^T(t_0) & w_2^T(t_0) & 0 \end{bmatrix}^T = \chi_0$, *has the following response:*

$$\begin{aligned} \chi(t) \;=\; & e^{\Lambda_o^k(t-t_j)}(M_k)^j\chi_0 + e^{\Lambda_o^k(t-t_j)}\sum_{i=0}^{j-1}(M_k)^i I_o\Gamma_{j-i} \\ & + \int_{t_j}^{t} e^{\Lambda_o^k(t-\tau)}Hd(\tau)d\tau \end{aligned} \tag{8}$$

for $t \in [t_j, \; t_{j+1})$, *with* $t_{j+1} - t_j = \Delta$, *where* $M_k = e^{\Lambda_o^k\Delta}$, $\Gamma_j = \int_0^\Delta e^{\Lambda_o^k\tau}Hd(t_j - \tau)d\tau$, $j = 1, 2, \cdots$, $I_o = \begin{bmatrix} I_{n\times n} & O & O & O \\ O & I_{n\times n} & O & O \\ O & O & I_{(n-q)\times(n-q)} & O \\ O & O & O & O \end{bmatrix}$, *I is the identity matrix.*

Having characterized the fault-free closed-loop response in terms of the sampling period, we are in a position to state the main result of this section. The following theorem provides a necessary and sufficient condition for practical stability and ultimate boundedness of the closed-loop plant under the sampled-data control structure.

Theorem 1: Consider the closed-loop system of Eqs.2-3 under continuous measurement sampling, where F^k *and* L *are chosen to enforce an ultimate bound* $r_k > 0$ *on the closed-loop state for any disturbance satisfying* $\| d(t) \| \leq D$ *for all* $t \geq 0$, *for any given* $D > 0$. *Next, consider the system of Eqs.6-7 with the initial condition* $\chi(t_0) = \begin{bmatrix} x^T(t_0) & \eta^T(t_0) & w_2^T(t_0) & 0 \end{bmatrix}^T := \chi_0$. *If the eigenvalues of the matrix* $M_k = e^{\Lambda_o^k\Delta}$ *lie strictly inside the unit circle, then given any positive real number* $\delta_k > r_k$, *there exists*

$\Delta^* > 0$, *such that if* $0 < \Delta \leq \Delta^*$, *the state of the sampled-data closed-loop system satisfies* $\limsup_{t\to\infty} \| \chi(t) \| \leq \delta_k$.

Proof: Evaluating the norm of the solution described in Proposition 1, we have from Eq.8 that for $t \in [t_j,\ t_{j+1}),\ j = 0, 1, 2, \cdots$:

$$\| \chi(t) \| \leq \| e^{\Lambda_o^k (t-t_j)} (M_k)^j \chi_0 \| + \| \int_{t_j}^{t} e^{\Lambda_o^k (t-\tau)} H d(\tau) d\tau \| + \| e^{\Lambda_o^k (t-t_j)} \sum_{i=0}^{j-1} (M_k)^i I_o \Gamma_{j-i} \| \quad (9)$$

Following [13], it can be shown that if the eigenvalues of M_k lie inside the unit circle (i.e., $\| (M_k)^j \| \leq \widehat{\alpha}_k e^{-\widehat{\beta}_k j}$, for some $\widehat{\alpha}_k, \widehat{\beta}_k > 0$), then the first term on the right hand side of Eq.9 satisfies the following bound:

$$\| e^{\Lambda_o^k (t-t_j)} (M_k)^j \chi_0 \| \leq \alpha_k e^{-\beta_k (t-t_0)} \cdot \| \chi_0 \| \quad (10)$$

where $\alpha_k = \widetilde{\alpha}_k \widehat{\alpha}_k e^{\widehat{\beta}_k} = e^{\sigma_k \Delta} \widehat{\alpha}_k e^{\widehat{\beta}_k}$, σ_k is the largest singular value of Λ_o^k, and $\beta_k = \widehat{\beta}_k / \Delta > 0$. Analyzing the third term on the right hand side of Eq.9, we obtain:

$$\| e^{\Lambda_o^k (t-t_j)} \sum_{i=0}^{j-1} (M_k)^i I_o \Gamma_{j-i} \| \leq \widetilde{\alpha}_k \sum_{i=0}^{j-1} \widehat{\alpha}_k e^{-\widehat{\beta}_k i} \| \Gamma_{j-i} \| \quad (11)$$

where we have used the fact that $\| I_o \| = 1$, $\| e^{\Lambda_o^k (t-t_j)} \| \leq \widetilde{\alpha}_k$, $\| (M_k)^i \| \leq \widehat{\alpha}_k e^{-\widehat{\beta}_k i}$, and $\| \Gamma_{j-i} \|$ is given by:

$$\begin{aligned} \| \Gamma_{j-i} \| &\leq \int_0^{\Delta} \| e^{\Lambda_o^k \tau} \| \| H \| \| d(t_{j-i} - \tau) \| d\tau \\ &= \frac{e^{\sigma_k \Delta} - 1}{\sigma_k} \| H \| D = \frac{\widetilde{\alpha}_k - 1}{\sigma_k} \| H \| D := \Gamma \end{aligned} \quad (12)$$

Substituting the last estimate into Eq.11 yields:

$$\begin{aligned} \| e^{\Lambda_o^k (t-t_j)} \sum_{i=0}^{j-1} (M_k)^i I_o \Gamma_{j-i} \| &\leq \widetilde{\alpha}_k \Gamma \sum_{i=0}^{j-1} \widehat{\alpha}_k e^{-\widehat{\beta}_k i} \\ &= \widetilde{\alpha}_k \widehat{\alpha}_k \Gamma \left(\frac{1 - (e^{-\widehat{\beta}_k})^j}{1 - e^{-\widehat{\beta}_k}} \right) \\ &\leq \frac{\widetilde{\alpha}_k \widehat{\alpha}_k \Gamma}{1 - e^{-\widehat{\beta}_k}} \end{aligned} \quad (13)$$

where we have used the fact that for $\widehat{\beta}_k > 0$, $0 < e^{-\widehat{\beta}_k} < 1$ and $\lim_{j\to\infty} (e^{-\widehat{\beta}_k})^j = 0$. With Eq.12 in mind, the second term on the right hand side of Eq.9 can be similarly bounded:

$$\| \int_{t_j}^{t} e^{\Lambda_o^k (t-\tau)} H d(\tau) d\tau \| \leq \frac{\widetilde{\alpha}_k - 1}{\sigma_k} \| H \| D = \Gamma \quad (14)$$

Combining Eqs.10, 13 and 14, we conclude that for $t \in [t_j, t_{j+1})$, and as $j \to \infty$:

$$\| \chi(t) \| \leq \alpha_k e^{-\beta_k t} \cdot \| \chi_0 \| + \frac{\widehat{\alpha}_k \widetilde{\alpha}_k \Gamma}{1 - e^{-\widehat{\beta}_k}} + \Gamma \quad (15)$$

and consequently $\lim_{t\to\infty} \| \chi(t) \| \leq \left(\frac{\widehat{\alpha}_k \widetilde{\alpha}_k}{1 - e^{-\widehat{\beta}_k}} + 1 \right) \Gamma := \delta_k'(\Delta)$, which implies that the sampled-data closed-loop states are ultimately bounded if the eigenvalues of M_k are within the unit circle. Let r_k be the ultimate bound under continuous communication (i.e., when $\Delta = 0$), then from the continuity of δ' with respect to Δ, it follows that given any $\delta_k > r_k$ there exists Δ^* such that $\delta_k'(\Delta) \leq \delta_k$ for $\Delta \in (0, \Delta^*]$, and therefore $\lim_{t\to\infty} \| \chi(t) \| \leq \delta_k$. ■

C. Application to the SOFC plant

To robustly regulate the stack temperature of the SOFC plant described in Section III in the absence of faults, an output feedback controller of the form of Eq.3 is designed where the controller gains for the three control configurations are chosen as $F^1 = \begin{bmatrix} -0.9853 & 0 & 0 & 10.9306 \end{bmatrix}$, $F^2 = \begin{bmatrix} 0 & -0.0314 & 0 & 19.7681 \end{bmatrix}$, and $F^3 = \begin{bmatrix} 0 & 0 & 0 & -10.7559 \end{bmatrix}$, and the observer gain is chosen such that the poles of $\widehat{A} - LC$ are placed at $(-0.1,\ -0.06,\ -1,\ -0.05)$ to enhance the speed at which the fuel cell meets the desired temperature set-point and to account for the time-varying external disturbances. To investigate the effect of model uncertainty on the stability of the sampled-data SOFC plant, we consider as an example parametric uncertainty in Cp_{H_2} and define $\delta_1 = (Cp_{H_2}^m - Cp_{H_2})/Cp_{H_2}$, where $Cp_{H_2}^m$ is a nominal value used in the model, as a measure of model accuracy (any other set of uncertain parameters can also be considered and analyzed in a similar fashion).

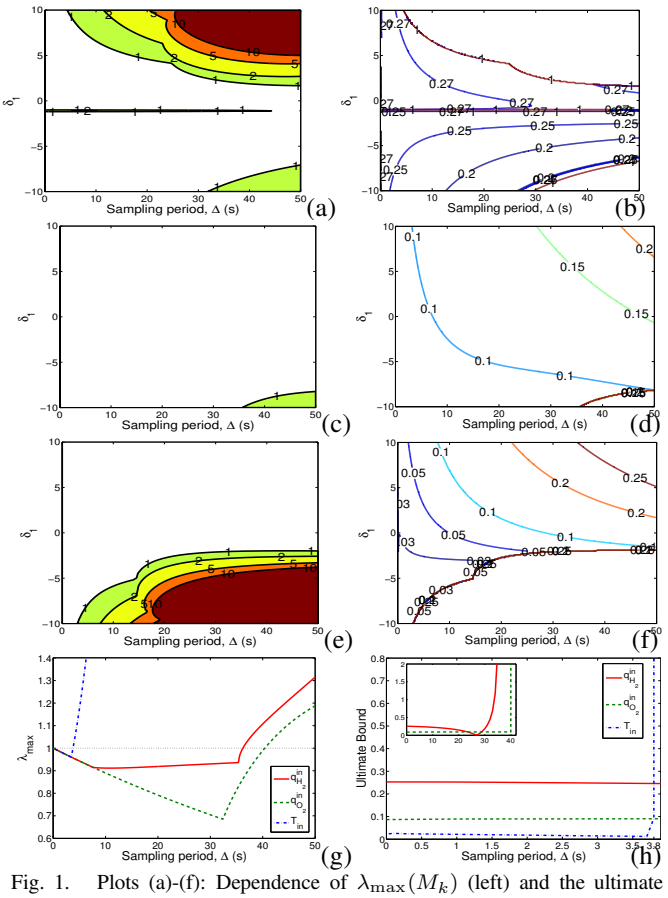

Fig. 1. Plots (a)-(f): Dependence of $\lambda_{\max}(M_k)$ (left) and the ultimate bound (right) on the plant-model mismatch and the sampling period when the manipulated input is chosen to be: (a)-(b) the inlet fuel flow rate, (c)-(d) the inlet air flow rate, and (e)-(f) the inlet temperature. Plots (g)-(h): Dependence of $\lambda_{\max}(M_k)$ (left) and the ultimate bound (right) on the sampling period for the three different control configurations when an inter-sample model predictor with $\delta_1 = -9$ is used.

Figs.1(a)-1(f) are contour plots that depict the dependence of the maximum eigenvalue magnitude of the matrix M_k (left) and the ultimate bound (right) – i.e., the disturbance attenuation level – on both δ_1 and the sampling period for

each of the three candidate control configurations in the fuel cell system. In plots (a), (c) and (e), the area enclosed by the unit contour lines in each plot (unshaded area) represents the stability region of the linearized plant within which the sampled-data closed-loop plant can be robustly stabilized under a given control configuration, while in plots (b), (d) and (f) the value of each contour line represents an upper bound on the size of the terminal set that the closed-loop plant state converges to when the values for δ_1 and Δ are chosen within the zone enclosed by that contour line. As expected, in general the range of tolerable parametric uncertainty shrinks as the sampling period is increased. It can also be seen that the control configuration with the inlet air flow rate as the manipulated input possesses the largest stability region of the three configurations. Additionally, for a given terminal set, the range of feasible sampling periods shrinks as the plant-model mismatch increases. Also, for a given plant-model mismatch, the size of the terminal set in general grows as the sampling period is increased. These trends are also depicted in Figs.1(g)-1(h), which show, respectively, $\lambda_{\max}(M_k)$ and the ultimate bound versus the sampling period for the three control configurations when a fixed inter-sample model predictor with $\delta_1 = -9$ is used. It is clear from Fig.1(g) that the different control configurations yield different maximum allowable sampling periods, with configuration 2 (dashed profile) requiring the lease frequent sampling, and configuration 3 requiring the fastest sampling (dash-dotted profile) with the maximum allowable sampling period $\Delta = 3.7$ s. Also, Fig.1(h) predicts that for $\Delta = 3.8$ s, the plant state will converge to a smaller terminal set with configuration 2 than with configuration 1. These predictions are further confirmed by the closed–loop temperature and manipulated input profiles in Fig.2 which show that the plant with the inlet temperature as the manipulated input (configuration 3) is unstable when the control system is operated with a sampling period of $\Delta = 3.8$ s (dotted profiles), which is greater than its maximum allowable sampling period, while the plant is stable under the other two configurations. However, the control configuration with the inlet air flow rate as the manipulated input (configuration 2) exhibits a better disturbance handling capability than the configuration with the inlet fuel flow rate as the manipulated input (configuration 1), since it achieves a smaller ultimate bound on the closed-loop plant state (solid). These results are consistent with Figs.1(g)-1(h). In obtaining these plots, a time-varying pulse disturbance (with an amplitude of 10% of the nominal value) was introduced into the load current after 1000 s (see Fig.2(d)).

V. Robust Fault Detection and Control System Reconfiguration

In this section, we use the fault-free closed-loop behavior characterized in the previous section as the basis for deriving appropriate rules for robust fault detection and reconfiguration. The idea is to use the state observer in Eq.5 as a fault detection filter and to compare its output with the actual output of the system at the sampling times to determine the fault or health status of the control actuators.

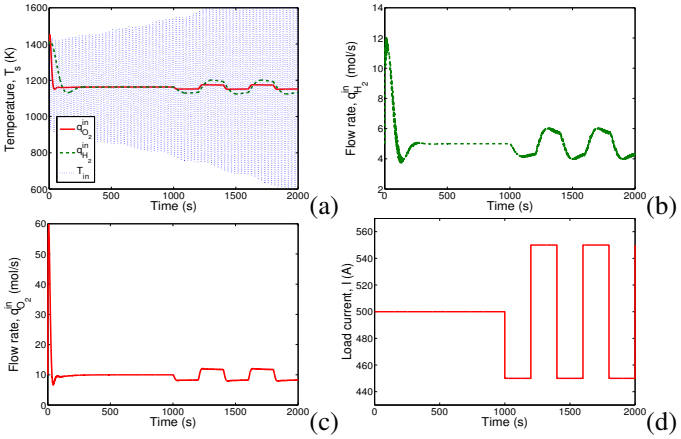

Fig. 2. Plot (a): Fuel cell stack temperature under the sampled-data control system with model uncertainty $\delta_1 = -9$ and a sampling period of $\Delta = 3.8$ s, with the inlet air flow rate (solid), the inlet fuel flow rate (dashed), and the inlet temperature (dotted) as the manipulated input. Plots (b)-(c): the manipulated input profiles. Plot (d): a disturbance in the load current.

A. Robust fault detection

Consider the closed-loop system of Eq.2 and Eq.5, for a fixed fault-free control configuration, $k \in \mathcal{K}$, with $f_a^k \equiv 0$, and consider the augmented system of Eqs.6-7 where the sampling period Δ is chosen such that $\lambda_{\max}(M_k) < 1$ and $\Delta \leq \Delta^*$ (from Theorem 1). Then the residual defined by $r_d = \|y - C\eta\|$ can be shown to satisfy a time-varying bound of the following form for all $t \geq t_0$:

$$r_d(t) \leq \bar{\alpha}_k \| \chi_0 \| e^{-\bar{\beta}_k(t-t_0)} + \bar{\delta}_k(\Delta, D, F^k, L) \qquad (16)$$

where $\bar{\alpha}_k = 2\|C\|\alpha_k$, $\bar{\beta}_k = \beta_k$ and $\bar{\delta}_k = 2\|C\|\ \delta'_k$. This bound can be obtained from the fact that $\|x(t)\| \leq \|\chi(t)\|$, $\|\eta(t)\| \leq \|\chi(t)\|$, and the fact that $\chi(t)$ satisfies Eq.15 in the absence of faults. Based on this result, and for a given sampling rate (which is robustly stabilizing in the absence of faults), the bound given in Eq.16 can be used as a time-varying alarm threshold, and a fault can be declared at any sampling time that the residual breaches this threshold, i.e.,

$$r_d(T_d) > \bar{\alpha}_k \| \chi_0 \| e^{-\bar{\beta}_k(T_d - t_0)} + \bar{\delta}_k \Longrightarrow f_a^k(T_d) \neq 0$$

for some $T_d > 0$. Note that this threshold accounts for the disturbances (recall that δ'_k depends on the size of the disturbance), and therefore any breach of this threshold cannot be attributed to the disturbances. Note also that even though the threshold is enlarged (relative to the disturbance-free case where $r_d(t)$ is bounded only by the exponentially-decaying term), the threshold can be tightened as desired by proper selection of the controller and observer design parameters (as well as the sampling period) to ensure a sufficiently small δ'_k and minimize detection delays. The underlying idea here is that by designing the sampled-data control system to achieve an arbitrary degree of disturbance attenuation in the absence of faults, the residual threshold can be made practically less sensitive to the disturbances, and responsive only to the faults. Furthermore, possible detection delays due to sampling can be reduced by properly tuning the controller and observer design parameters to ensure that the constants $\bar{\alpha}_k$ and $\bar{\beta}_k$ are sufficiently tight; however,

the smallest possible delay is ultimately constrained by the feasible sampling rate.

B. Control system reconfiguration logic

Once a fault is detected in the operating control configuration, the local control system needs to determine which fall-back configuration to select and activate in order to preserve closed-loop stability and ensure fault-tolerance. Specifically, consider the closed-loop system of Eq.2 and Eq.5, with $k(t_0) = i$ for some $i \in \mathcal{K}$ and a sampling period Δ such that $\lambda_{\max}(M_k) < 1$ and $\Delta \leq \Delta^*$. Let T_d be the earliest time that a fault is detected. Then the following switching rule:

$$k(t) = \left\{ \begin{array}{ll} i, & 0 \leq t < T_d \\ \nu \neq i, & t \geq T_d,\ \lambda_{\max}(M_\nu) < 1, \\ & \delta_\nu(\Delta) \leq \delta_l(\Delta),\ \forall\, l \in \mathcal{K} \setminus \{i\} \end{array} \right\} \quad (17)$$

guarantees that the control system switches to a control configuration that: (1) is robustly stabilizing for the given sampling period, and (2) enforces the largest degree of disturbance attenuation among all the feasible backup candidates. Note that a similar logic can be applied to the case when multiple consecutive faults take place. Following any reconfiguration event, however, a new residual alarm threshold needs to be observed and implemented to allow the detection of future possible faults in the new configuration. Furthermore, in cases where none of the backup control configurations satisfies the stability and performance conditions in Eq.17, the problem can be addressed either by adjusting the controller/observer design parameters (i.e., switching the controller and observer gains to values for which at least one backup configuration is stabilizing) or by switching to alternative sensors that have the required sampling period.

C. Application to the SOFC plant

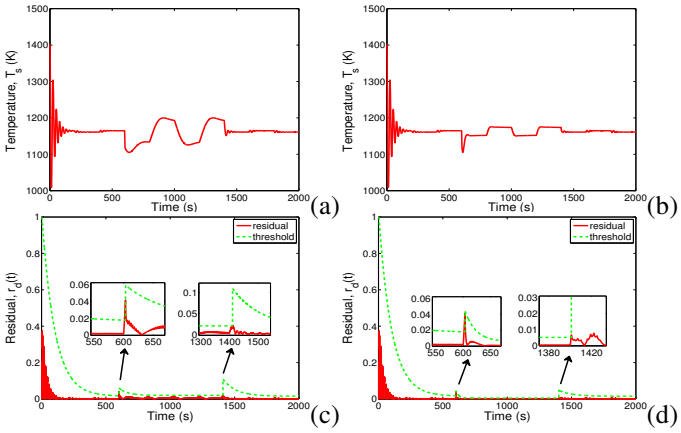

Fig. 3. Evolution of the fuel cell stack temperature and fault detection filter residual under two consecutive faults, at $T_{f1} = 600$ s and $T_{f2} = 1400$ s, and subsequent switching from configuration 3 to 1 to 3 (plots (a) and (c)), and switching from configuration 3 to 2 to 3 (plots (b) and (d)).

To illustrate the implementation of the switching logic in situations where more than one backup configuration is stabilizing, the plant is initialized using configuration 3 with $\Delta = 3$ s (this forces the state to converge to the smallest terminal set as predicted by Fig.1(h)), in the presence of a pulse disturbance in I with an amplitude of 10% of the nominal value. An inter-sample model predictor with $\delta_1 = -9$ is used to estimate the evolution of the output between sampling instances. A fault is introduced at $T_{f1} = 600$ s and is detected shortly thereafter at $T_{d1} = 603$ s. In deciding which backup control configuration should be activated at this time, it can be observed from Fig.1(g) that, for the given sampling period, both backup configurations can robustly stabilize the closed-loop system since $\lambda_{\max}(M_1) < 1$ and $\lambda_{\max}(M_2) < 1$. However, according to Fig.1(h), control configuration 2 exhibits a smaller ultimate bound (and thus a greater level of disturbance attenuation) at the operating sampling rate than does control configuration 1. This prediction is further confirmed by the stack temperature profiles shown in Figs.3(a)-(b) in which a time-varying pulse disturbance is introduced in the load current. It can been that the closed-loop system that is reconfigured to configuration 2 (plot (b)) exhibits better disturbance attenuation capability than the one switched to configuration 1 (plot (a)). Following the activation of the new control configuration, a new fault is introduced in the backup configuration at $T_{f2} = 1400$ s and is detected immediately, and the control system then switches back to configuration 3 (which is assumed to have been repaired by this time). Note from the residual profiles in Figs.3(c)-(d) that a new alarm threshold is used following reconfiguration (see dashed lines).

REFERENCES

[1] P. A. Daly and J. Morrison, "Understanding the potential benefits of distributed gen-eration on power delivery systems," in *Proceedings of Rural Electric Power Conference*, Little Rock, AK, 2001, pp. 1–13.

[2] A. Borbely and J. F. Kreider, *Distributed Generation: The Power Paradigm of the New Millennium*. Boca Raton, FL: CRC Press, 2001.

[3] K. Tomsovic and T. Hiyama, "Intelligent control methods for systems with dispersed generation," in *Proceedings of IEEE Power Engineering Society Winter Meeting*, Columbus, OH, 2001, pp. 913–917.

[4] F. Jurado and J. Saenz, "Adaptive control of a fuel cell-microturbine hybrid power plant," in *Proceedings of IEEE Power Engineering Society Summer Meeting*, Chicago, IL, 2002, pp. 76–81.

[5] M. Marwali and A. Keyhani, "Control of distributed generation systems-part I: Voltages and currents control," *IEEE Transactions on Power Electronics*, vol. 19, pp. 1541–1550, 2004.

[6] K. Sedghisigarchi and A. Feliachi, "Dynamic and transient analysis of power distribution systems with fuel cells-part II: control and stability enhancement," *IEEE Transactions on Energy Conversion*, vol. 19, pp. 429–434, 2004.

[7] M. Arcak, H. Gorgun, L. Pedersen, and S. Varigonda, "A nonlinear observer design for fuel cell hydrogen estimation," *IEEE Trans. Contr. Syst. Techn.*, vol. 12, pp. 101–110, 2004.

[8] A. L. Dimeas and N. D. Hatziargyriou, "Operation of a multiagent system for microgrid control," *IEEE Transactions on Power Systems*, vol. 20, pp. 1447–1455, 2005.

[9] R. Roberts, J. Brouwer, F. Jabbari, T. Junker, and H. Ghezel-Ayahg, "Control design of an atmospheric solid oxide fuel cell/gas turbine hybrid systems: Variable versus fixed speed has turbine operation," *Journal of Power Sources*, vol. 161, pp. 484–491, 2006.

[10] Y. Sun, S. Ghantasala, and N. H. El-Farra, "Networked control of distributed energy resources: Application to solid oxide fuel cells," *Ind. & Eng. Chem. Res.*, vol. 48, pp. 9590–9602, 2009.

[11] W. Qi, J. Liu, X. Chen, and P. D. Christofides, "Supervisory predictive control of stand-alone wind-solar energy generation systems," *IEEE Trans. Contr. Syst. Techn.*, vol. 19, pp. 199–207, 2011.

[12] Y. Sun, S. Ghantasala, and N. H. El-Farra, "Monitoring and fault-tolerant control of distributed power generation: Application to solid oxide fuel cells," in *Proceedings of American Control Conference*, Baltimore, MD, 2010, pp. 448–453.

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