AIChE WILEY InterScience DISCOVER SOMETHING GREAT

Fault-Tolerant Control of Nonlinear Process Systems Subject to Sensor Faults

Prashant Mhaskar
Dept. of Chemical Engineering, McMaster University, Hamilton, ON L8S 4L7, Canada

Adiwinata Gani, Charles McFall, Panagiotis D. Christofides, and James F. Davis
Dept. of Chemical & Biomolecular Engineering, University of California, Los Angeles, CA 90095

DOI 10.1002/aic.11100
Published online February 6, 2007 in Wiley InterScience (www.interscience.wiley.com).

The problem of control of nonlinear process systems subject to input constraints and sensor faults (complete failure or intermittent unavailability of measurements) is considered. A fault-tolerant controller is designed that utilizes reconfiguration (switching to an alternate control configuration) in a way that accounts for the process nonlinearity, the presence of constraints and the occurrence of sensor faults. To clearly illustrate the importance of accounting for the presence of input constraints, first the problem of sensor faults that necessitate sensor recovery to maintain closed-loop stability is considered. We address the problem of determining, based on stability region characterizations for the candidate control configurations, which control configuration should be activated (reactivating the primary control configuration may not preserve stability) after the sensor is rectified. We then consider the problem of asynchronous measurements, that is of intermittent unavailability of measurements. To address this problem, the stability region (that is, the set of initial conditions starting from where closed-loop stabilization under continuous availability of measurements is guaranteed), as well as the maximum allowable data loss rate which preserves closed-loop stability for the primary and the candidate backup configurations are computed. This characterization is utilized in identifying the occurrence of a destabilizing sensor fault, and in activating a suitable backup configuration that preserves closed-loop stability. The proposed method is illustrated using a chemical process example and demonstrated via application to a polyethylene reactor. © 2007 American Institute of Chemical Engineers *AIChE J,* 53: 654–668, 2007

Keywords: Fault-tolerant control, sensor data losses, input constraints, stability region, Lyapunov-based control

Introduction

Safe and profitable operation of chemical plants relies, among other things, on controller designs that account for the inherently complex dynamics of the processes (manifested as nonlinearities), operational issues, such as constraints and uncertainties, as well as abnormalities (arising, for example, due to faults in sensors/actuators). The interconnected nature of chemical processes puts a greater emphasis on handling these issues to avoid propagation of the faults and causing entire plant shutdowns or safety hazards. These considerations motivate development of control strategies that account for constraints, nonlinearities, uncertainty, as well as are tolerant to faults (fault-tolerant control). Fault-tolerant control has

Correspondence concerning this article should be addressed to P. D. Christofides at pdc@seas.ucla.edu.

been an active area of research for the past ten years, and has motivated many research studies in the context of aerospace engineering applications (see, for example,[3,47]).

The ability to implement fault-tolerant control relies on some degree of redundancy in the control configurations (availability of sets of sensor/actuator combinations that can be used to implement controllers), that can either be used all at one time (the reliable control approach, for example,[21]), or activated when the need arises (the reconfiguration approach). The use of only as many control loops as required at a time is motivated by economic considerations (to save on unnecessary control action), and has been employed in the context of chemical processes; however, the available results are mostly based on the assumption of a linear system description (for example,[8,22]), and do not account for complexities such as control constraints.

In implementing fault-tolerant control (as well as feedback control), the importance of sensors is well-recognized and several researchers have focused on the problem of efficient sensing and measurement for well-functioning sensors and networks of sensors.[9,18,19] In[4,5,17,27] the problem of measurements arriving at different known rates, and its implication on simulation and control (multirate control) is addressed. In chemical processes, sensor data losses arising due to sampling, measurement or communication irregularities are more likely to be manifested as intermittent availability of measurements (asynchronous measurements), where only an average rate of availability of measurements is known, but not the exact times when the measurements will be available.

When explicitly considered, irregular measurements can be analyzed as a robustness problem. Specifically, for a given stabilizing control law, a bound on the sensor data loss rate (defined as the ratio of the time during which measurements are available over the total time) can be computed such that if the sensor data loss rate is within this bound, closed-loop stability is preserved. The difference in the nature of sensor irregularities (measurements arriving at different known rates as opposed to asynchronously) has important implications in the robustness of a given system to sensor data losses. Furthermore, for unconstrained systems, such a bound for the data loss rate (defined over an infinite time interval) can be computed (for example, see[6,48] and the references therein). For constrained systems, however, for such a bound on the data loss rate to exist, it has to be defined over a finite time interval where the derived bound accounts for the limitations imposed by the presence of constraints.

The extensive work in the area of nonlinear process control can be utilized toward computing such a bound, and in choosing the appropriate feedback law (for excellent reviews of results in the area of nonlinear process control see[7,23,49,50]; for a more recent review see[51]). These approaches have recently been utilized to address the problem of fault-tolerant control of nonlinear processes subject to constraints and faults in the control actuators. In[44] a reconfiguration-based approach was utilized for the purpose of achieving tolerance to actuator faults under the assumptions that the measurements were continuously available. In[45,52] sensor faults arising due to communication losses were modeled as delays in implementing the control action and a reconfiguration strategy was devised to achieve fault-tolerance subject to faults in the control actuators. The results of[44,45] however, do not take the presence of intermittent sensor data losses into account either in the implementation of individual control configurations, or in the reconfiguration strategies. The fault-tolerant (or even stabilizability in the absence of faults) capabilities of the results of[44,45] therefore, do not hold in the presence of sensor data losses. Furthermore, outside of these recent results as well the problem of fault-tolerant control for handling sensor faults for nonlinear systems subject to constraints in the control actuators has received limited attention.

Motivated by the above, in this work we consider the problem of fault-tolerant control of non-linear process systems subject to input constraints and sensor faults (both complete failures and asynchronous measurements). We employ a reconfiguration-based approach, wherein, for a given process, a set of candidate control configurations are first identified, and in the event of a fault an appropriate backup configuration is activated to maintain stability. To illustrate the importance of accounting for the presence of constraints, we first consider sensor faults manifested as complete loss of measurements (faults that necessitate taking corrective action to repair the sensors). We address the problem of determining which candidate control configuration should be implemented in the closed-loop system to achieve stability after the sensor is recovered (this analysis is carried out under the assumption of continuous availability of measurements when the sensor is functioning). We then consider the problem in the presence of intermittent sensor data losses. We define the sensor data loss rate to account for the presence of constraints (specifically, we define the data loss rate over a finite time interval), and analyze the stability properties in the presence of input constraints and sensor data losses. We characterize the stability region (that is, the set of initial conditions starting from where closed-loop stabilization under continuous availability of measurements is guaranteed) and the maximum allowable data loss rate that a given control configuration can tolerate. If the data loss rate goes above the allowable data loss rate, reconfiguration is triggered and a candidate backup configuration is activated for which the state of the closed-loop system resides in the stability region of the candidate configuration, and the data loss rate is less than the allowable data loss rate for the candidate control configuration. We use a chemical reactor example to illustrate our method and then demonstrate an application to a polyethylene reactor.

Preliminaries

We consider nonlinear processes with input constraints, described by

$$\begin{aligned}
\dot{x} &= f(x) + G_{k(t)}(x)u_{k(t)}(y(t)) \\
y(t) &= \left\{ \begin{array}{ll} x(t) & t \in [t_{2i}, t_{2i+1}) \\ x(t_{2i+1}) & t \in [t_{2i+1}, t_{2i+2}) \end{array} \right\} \\
& u_k \in \mathrm{U}_k, k(t) \in \mathcal{K} = \{1, \ldots, N\},\ N < \infty
\end{aligned} \tag{1}$$

where $x \in \mathbb{R}^n$ denotes the vector of state variables, $y \in \mathbb{R}^n$ denotes the vector of measured variables, $[t_{2i}, t_{2i+1})$ and $[t_{2i+1}, t_{2i+2})$ denote the time intervals during which measurements of the state variables are available, and are lost, respectively, with $t_0 = 0$ (that is, measurement being initially available), $u_{k(t)}(y(t)) \in \mathrm{IR}^m$ denotes the manipulated inputs under the kth configuration taking values in a nonempty convex subset $\mathbf{U}_k$ of IR^m, where $\mathbf{U}_k = \{u \in \mathrm{IR}^m : \|u\| \le u_k^{max}\}$, $\|\cdot\|$ is the Euclidean norm of a vector, $u_k^{max} > 0$ is the magnitude of input constraints and $f(0) = 0$. The vector function $f(x)$, and the matrix $G_k(x) = [g_{1,k}(x) \cdots g_{m,k}(x)]$ are assumed to be sufficiently smooth on their domains of definition. $k(t)$, which takes values in the finite index set $\mathcal{K}$, represents a discrete state that indexes the matrix $G_k(\cdot)$, as well as the manipulated input $u_k(\cdot)$. For each value that k assumes in $\mathcal{K}$, the system is controlled via a different set of manipulated inputs which defines a given control configuration. The notation $L_f h$ denotes the standard Lie derivative of a scalar function $h(\cdot)$ with respect to the vector function $f(\cdot)$, and the notation $x(T^-)$ denotes the limit of the trajectory $x(t)$ as T is approached from the left, that is, $x(T^-) = \lim_{t \to T^-} x(t)$. Throughout the manuscript, we assume that for any $u_k \in \mathbf{U}_k$ the solution of the system of Eq. 1 exists and is continuous for all t.

We next review one example of a state feedback controller[40,41] (inspired by the results on bounded control in[13]) that, under the assumption of continuous availability of measurements, provides an explicit estimate of the stability region for the closed-loop system subject to constraints (for more details on the controller design, and the proof, see[40,41]).

Theorem 1[41]: *Consider the nonlinear system of Eq. 1 under state feedback (that is, x(t) is available for all t ≥ 0) for a configuration k, for which a Control Lyapunov Function V_k exists, under the following bounded nonlinear feedback controller*

$$u_k = -w_k(x, u_k^{max})(L_{G_k} V_k(x))^T \tag{2}$$

where $w_k(x, u_k^{max}) =$

$$\begin{cases} \dfrac{\alpha_k(x) + \sqrt{\alpha_k^2(x) + (u_k^{max}\|b_k^T(x)\|)^4}}{\|b_k^T(x)\|^2 \left[1 + \sqrt{1 + (u_k^{max}\|b_k^T(x)\|)^2}\right]}, & b_k^T(x) \neq 0 \\ 0, & b_k^T(x) = 0 \end{cases} \tag{3}$$

with $\alpha_k(x) = L_{f_k} V_k(x) + \rho_k V_k(x)$, $\rho_k > 0$ and $b_k(x) = L_{G_k} V_k(x)$. Assume that the set $\Phi_k(u_k^{max})$ of x satisfying

$$L_{f_k} V_k(x) + \rho_k V_k(x) \le u_k^{max} \|(L_{G_k} V_k(x))^T\| \tag{4}$$

contains the origin and a neighborhood of the origin. Also, let $\Omega_k(u_k^{max}) := \{x \in \mathrm{IR}^n : V_k(x) \le c_k^{max}\}$ be a level set of V_k, completely contained in Φ_k, for some $c_k^{max} > 0$. Then for all $x(0) \in \Omega_k(u_k^{max})$ the control law of Eqs. 2–4 guarantees that the origin of the closed-loop system is asymptotically stable.

Remark 1: The problems caused by input constraints have motivated numerous studies on the dynamics and control of systems subject to input constraints. Important contributions include results on optimization-based methods such as model predictive control (for example,[1,2,23]) and Lyapunov-based control (for example,[10,13,14,24]). Stabilizing control laws that provide explicitly-defined regions of attraction for the closed-loop system have been developed using Lyapunov techniques; the reader may refer to[24] for a survey of results in this area. Recently, we developed a hybrid predictive control structure that employs switching between bounded control and MPC for stabilization of nonlinear systems,[37] and nonlinear systems with uncertainty,[46] subject to input constraints via using Lyapunov-based controllers[40,41] as fall-back controllers. More recently Lyapunov-based model predictive controllers were designed that guarantee stabilization from an explicitly characterized set of initial conditions in the presence of input[42] and input and state[43] constraints. The controller of Eq. *3* is one example of a controller design that provides an explicit characterization of the stability region in the presence of input constraints, and is only used to illustrate the main ideas behind the proposed approach. The results in this work are not limited to this particular controller design, and any other controller design that provides an explicit characterization of the stability region can be used instead (for example, the hybrid predictive controller[37,46] or the Lyapunov-based predictive controller[42,43]) for further details and references, see.[51]

Chemical reactor example

In this section, we describe a chemical reactor that we will use to illustrate the key features of the proposed method. To this end, consider a well-mixed, non-isothermal continuous stirred-tank reactor where three parallel irreversible elementary exothermic reactions of the form $A \overset{k_1}{\rightarrow} B$, $A \overset{k_2}{\rightarrow} U$ and $A \overset{k_3}{\rightarrow} R$ take place, where A is the reactant species, B is the desired product and U, R are undesired byproducts. The feed to the reactor consists of pure A at flow rate F, molar concentration C_{A0}, and temperature T_{A0}. Due to the non-isothermal nature of the reactions, a jacket is used to remove/provide heat to the reactor. Under standard modeling assumptions, a mathematical model of the process can be derived from material and energy balances and takes the following form

$$\begin{aligned} \frac{dT}{dt} &= \frac{F}{V}(T_{A0} - T) + \sum_{i=1}^{3} R_i(C_A, T) + \frac{Q}{\rho c_p V} \\ \frac{dC_A}{dt} &= \frac{F}{V}(C_{A0} - C_A) - \sum_{i=1}^{3} k_{i0} e^{-E_i/RT} C_A \end{aligned} \tag{5}$$

where $R_i(C_A, T) = \frac{(-\Delta H_i)}{\rho c_p} k_{i0} e^{\frac{-E_i}{RT}} C_A$, C_A denotes the concentrations of the species A, T denotes the temperature of the reactor, Q denotes the rate of heat input/removal from the reactor, V denotes the volume of the reactor, ΔH_i, k_i, E_i, $i = 1, 2, 3$, denote the enthalpies, pre-exponential constants and activation energies of the three reactions, respectively, c_p and ρ denote the heat capacity and density of fluid in the reactor. The values of the process parameters and the corresponding steady-state values and details of controller design can be found in.[29,44] It was verified that under these conditions, the system of Eq. 5 has three steady-states (two locally asymptotically stable and one unstable at $(T_s, C_{As}) = (388\ K, 3.59\ mol/L)$).

The control objective considered here is that of stabilizing the reactor at the (open-loop) unstable steady-state using the measurements of concentration and temperature. The following manipulated input candidates are assumed to be available (see Figure 1):

1. Configuration 1: Rate of heat input, $u_1 = Q$, subject to the constraints $|Q| \le u_{max}^1 = 748$ KJ/s.

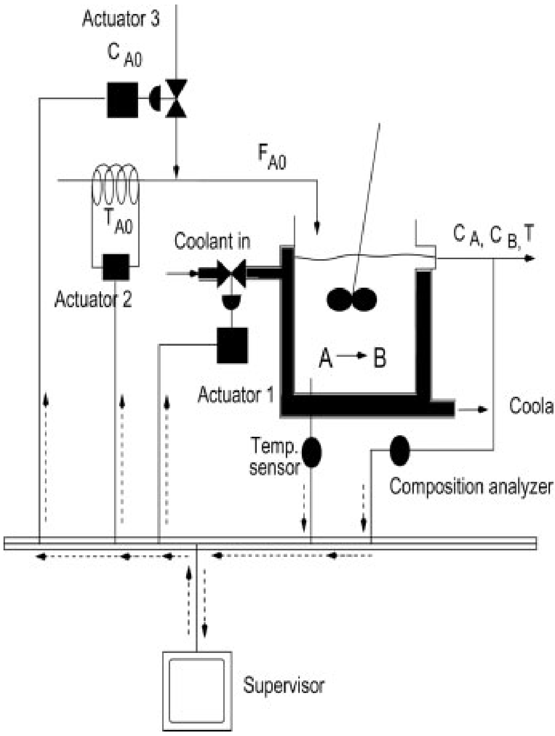

Figure 1. CSTR showing the three candidate control configurations.

2. Configuration 2: Inlet stream temperature, $u_2 = T_{A0} - T_{A0s}$, subject to the constraints $|u_2| \leq u^2_{max} = 100$ K.

3. Configuration 3: Inlet reactant concentration, $u_3 = C_{A0} - C_{A0s}$, subject to the constraints $|u_3| \leq u^3_{max} = 4$ mol/L.

Configuration 2 will be used as the primary manipulated input.

We will use this chemical reactor to motivate our results. To this end, we consider the chemical reactor operating under a given control configuration. At a certain time one of the sensors fails in a way that it is imperative to recover the sensor to implement feedback control. The problem that we analyze is whether reactivating the original control configuration (after sensor recovery) guarantees closed-loop stability. We will next consider the problem where the sensors do not fail, however, the process experiences intermittent loss of measurements (and this rate increases at a certain time due to sampling/measurement/communication errors). In this case, how much measurement data loss can be tolerated by the currently active control configuration, before it becomes necessary to reconfigure, and, if necessary, which backup configuration should be activated in the closed-loop system? Note that while we use the simple chemical reactor example only to motivate our results, the scenarios that we describe are relevant to all process operations. We also include an application to a more realistic process example, a polyethylene reactor, on the second example.

Stabilization subject to sensor failures

In this section, we consider the problem arising out of sensor failures that lead to the failure of the control loop and necessitate recovery. In analyzing this problem and in devising the fault-tolerant control strategy, we account for the presence of nonlinearity and constraints, and show how they impact the reconfiguration logic.

Reconfiguration law

Consider the closed-loop system of Eqs. 1–4 for which candidate control configurations have been identified and the stability region under each candidate configuration has been explicitly characterized. Let the closed-loop system of Eqs. 1–4 be initialized under a configuration k with $x_0 \in \Omega_k$. Let T^f be the time at which the sensor fails, and T^r be the time at which the sensor recovers. In the absence of measurements, the process runs open loop from the time T^f to T^r. Consequently, during this time the process state may drift further away from the desired operating condition. When the measurements become available again, switching to the original control configuration may not achieve closed-loop stability. The key consideration in devising the reconfiguration logic is the limitation imposed on the stability region under a given control configuration by the presence of input constraints and is formalized in Theorem 2.

Theorem 2: *Let $k(0) = i$ for some $i \in \mathcal{K}$ and $x(0) := x_0 \in \Omega_i$. Let T^f be the time that the sensor measurements become unavailable, and let T^r be the earliest time that they become available again. Then, the following switching rule*:

$$k(t) = \left\{ \begin{array}{ll} i, & 0 \leq t < T^f \\ l, & t \geq T^r, x(T^r) \in \Omega_l \end{array} \right\} \tag{6}$$

guarantees asymptotically stabilization of the origin of the closed-loop system.

Proof of Theorem 2: We consider the two possible cases; first if no sensor failure occurs ($T^f = \infty$), and second if a failure occurs at some finite time T^f and the sensors are recovered at time T^r.

Case 1: The absence of a failure implies $k(t) = i \; \forall \; t \geq 0$. Furthermore, since $x(0) \in \Omega_i$, and control configuration i is implemented for all times in this case, asymptotic stability follows from Theorem 1.

Case 2: At time T^r, the supervisor switches to a control configuration l for which $x(T^r) \in \Omega_l$. From this time onwards, since configuration l is implemented in the closed-loop system for all times, and since $x(T^f) \in \Omega_l$, once again, asymptotic stability follows from Theorem 1. This completes the proof of Theorem 2.

Remark 2: Theorem 2 accounts for the presence of constraints in the reconfiguration logic via the consideration of the stability region of candidate control configurations. Note that the problem that we consider here are sensor failures that result in loss of controllability. For the sake of illustration, consider a linear system of the form $\dot{x} = Ax + Bu$; $y = Cx$, where x is the state vector, y is the vector of measured variables, and u is the vector of manipulated variables, with A, B and C being matrices of appropriate dimensions. Consider the case when all state variables are being measured ($C = I$), and a state feedback law of the form $u = Ky = Kx$ is used to stabilize the system. Furthermore let some of the sensors fail at some time, resulting in a new C matrix denoted by $\overline{C}$. The same feedback gain matrix

K may no longer be stabilizing. If $\overline{C}$ is such that it can be used to reconstruct (estimate) the unstable states of the system (that is, all the unstable states remain observable) then feedback control (with an observer, and with a different feedback gain matrix) can still be used to stabilize the system. However if $\overline{C}$ is such that some of the unstable states of the system become unobservable, then the system simply cannot be stabilized using feedback control, and fixing the sensors becomes imperative. In other words, it is when measurements become unavailable (due to individual sensor malfunction, or loss of communication lines) that result in loss of controllability, that it becomes imperative to detect, isolate and correct the problem. Due to the open-loop behavior of the process during this intermediate time, the process states may drift and go out of the stability region of the currently active control configuration. Reactivating the original control configuration may, therefore, not stabilize the closed-loop system making it necessary to ascertain the suitability of a candidate control configuration by using Theorem 2 (see the simulation example for a demonstration).

Remark 3: While in this work we do not focus on the problem of fault-detection and isolation (considering instead the problem of determining the corrective action that needs to be taken once the fault information is available), this problem has been approached using a data-based or a model-based strategy. Statistical and pattern recognition techniques for data analysis and interpretation (for example,[15,16,20,25,33]), use past plant data to construct indicators that identify deviations from normal operation, and help in isolating faults. The problem of using fundamental process models for the purpose of detecting faults has been studied extensively in the context of linear systems[11,12,26]; and recently, some existential results in the context of nonlinear systems have been derived.[28–30]

In[44] we proposed an integrated fault-detection and fault-tolerant control structure that handles faults in the control actuators under the assumption of continuous availability of state or output measurements. The fault-detection filter in[44] relies on the measurements to observe deviations of the process behavior from the expected closed-loop behavior to detect faults, and needs to be redesigned if required to detect and isolate faults in the sensors. While the problem of designing sensor fault-detection and isolation filter remains outside the scope of this work, we note that the proposed fault-tolerant controller allows the use of any data- or model-based fault-detection and isolation filter to provide information about the occurrence of the fault (leading to its recovery). In this work, we focus instead on determining what corrective action needs to be taken after a fault has been reported and how the time that it takes to recover the fault impacts on the reconfiguration logic. Specifically, the reconfiguration logic points to the necessity of recovering the sensor sufficiently fast to avoid the situation where the process state, by the time of recovery, has escaped the stability region of the backup configurations. Alternatively, the proposed method can also be used for the purpose of designing the control configurations in a way that maximizes the region in state space covered by the backup configurations to increase the chances that the process state at the time of recovery lies in the stability region of at least one backup configuration.

Application to the chemical reactor

In this section, we illustrate the utility of the reconfiguration law of Eq. 6. To this end, consider the chemical reactor of Eq. 5 with the three candidate control configurations available. The first step in implementing the reconfiguration law of Eq. 6 is that of determining the stability regions of the individual control configurations under the control law of Eqs. 2–4. An explicit characterization of the stability regions is obtained and is shown in Figure 2. The area indicated by I, II and III indicates the set of initial conditions starting from where all three configurations can stabilize the closedloop system, I and II starting from where only configurations 1 and 2 can achieve stability, and I and III indicate the set of initial conditions starting from where only configurations 1 and 3 can stabilize the closed-loop system.

The closed-loop system is initialized under configuration 2 from an initial condition belonging to the stability region of configuration 2. At $t = 200$ min, however, a sensor failure occurs resulting in open-loop operation, and the process state begins to drift away from the desired equilibrium point (see dotted line in Figure 2). Recognizing that it is imperative to rectify this fault, the sensors are recovered (alternatively, redundant sensors are activated) at $t = 220$ min. With the state information again available, if the original control configuration (configuration 2) is reactivated, closed-loop stability is not achieved (see dash-dotted lines in Figure 2). This happens because during the time that the process was running open-loop, the states of the closed-loop system moved away from the desired equilibrium point, and out of the stability region of configuration 2. In contrast, if the reconfiguration

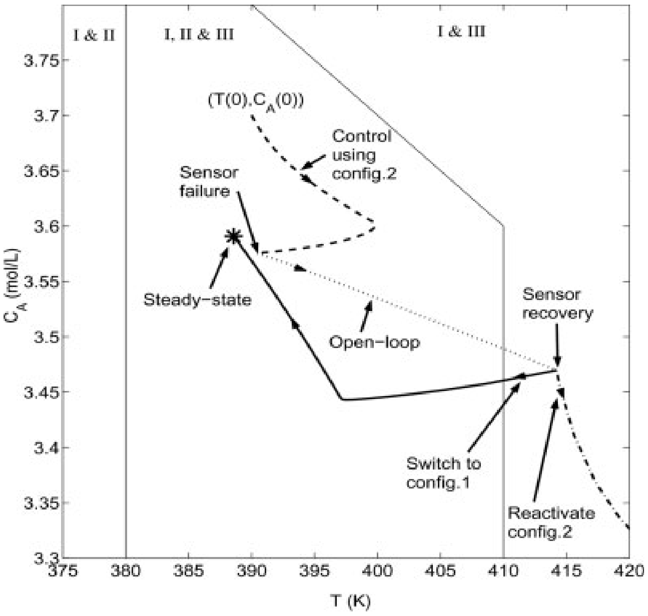

Figure 2. Evolution of the state profile under configuration 2 (dashed line) followed by loss of measurements (dotted line), and upon recovery reactivating configuration 2 (dash-dotted line), closed-loop stability is not preserved; however, switching to configuration 1 (solid line) preserves closed-loop stability.

law of Eq. 6 is used, the law dictates activation of configuration 1 (since the process state, when state information becomes available again, lies in the stability region of configuration 1). Closed-loop stability is subsequently achieved (solid line in Figure 2). Note that at the time the state information became available again, the state was also in the stability region of configuration 3, and switching to either configuration 1 or 3 would guarantee closed-loop stability. In such cases (when more than one control configurations satisfy the stability criteria), additional performance criteria, such as ease/cost of use can be used to decide which control configuration should be implemented in the closed-loop system.[38]

Stabilization subject to sensor data losses

In the previous section, we considered the problem of devising the reconfiguration law in a way that accounts for the presence of constraints on the manipulated inputs under the available control configurations. We now consider the problem of intermittent sensor data losses (not complete failures), and develop a reconfiguration law that achieves fault-tolerance in the presence of sensor data-losses. As evidenced in the previous section, a prerequisite to implementing fault-tolerant control is the characterization of the stability properties under the available control configurations, which we undertake in this section, and in the next section present the reconfiguration law. We consider the closed-loop system of Eqs. 1–4 under a configuration k, and drop the subscript k in the remaining of this section with the understanding that the robustness of the closed-loop system under control configuration k is being analyzed.

Modeling sensor data loss

Preparatory to the analysis of the stability properties of the closed-loop system under sensor data losses, we describe how we model the occurrence of sensor data losses. Specifically, sensor data availability is modeled as a random Poisson process. At a given time t an "event" takes place that determines whether the system will be closed-loop or open-loop (see Figure 3). For a given rate of data loss $0 \leq r \leq 1$, a random variable P is chosen from a uniform probability distribution between 0 and 1. If $P \leq r$, the event is deemed to be "measurement loss", while if $P > r$, the event is understood to be "measurement available". Furthermore, with W defined as the number of events per unit time, another random variable χ with uniform probability distribution between 0 and 1 determines the time for which the current event will last, given by $\Delta = \frac{-ln\chi}{W}$. At $t + \Delta$ another event takes place, and whether it represents a measurement or loss of measurement, as well as its duration, is similarly determined. Note that in the presence of constraints, prolonged duration of measurement loss may land the system states at a point starting from where stabilization may not be achievable (even with continuous measurement); in characterizing the stability properties of constrained systems, we therefore need to define data loss rates over a finite time interval as stated in assumption 1 below.

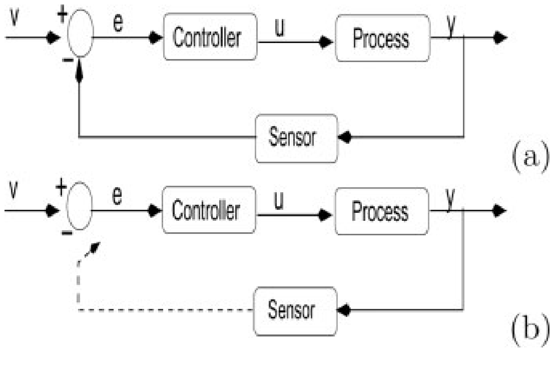

Figure 3. Closed-loop system in the (a) absence, and (b) presence of sensor data losses.

Assumption 1: *For a positive real number T^*, defining $r \in [0, 1]$ as the sensor data loss rate implies that over every successive finite time interval T^*, the measurements are available for a total time of $T^* \times (1 - r)$.*

Note that assumption 1 does not impose any restrictions on the distribution of sequences of measurement loss and availability over the time interval T^*. Furthermore, the assumption does not need to hold for *any* finite interval T^*, but only successive time intervals T^*. To illustrate the difference, consider the case where the assumption requires the data loss rate to hold over any finite time interval T^*, and that one such interval is τ, $\tau + T^*$. Requiring the data loss rate to hold over any interval T^* would mean that the same data loss rate should also hold over the interval $\tau + \varepsilon_t$, $\tau + T^* + \varepsilon_t$, for *any* positive real number ε_t, which can only be true if the data loss and measurement events are periodic with a period T^*. The requirement that the data loss rate hold over successive intervals T^* only says that over the time interval T^*, if the duration of all the measurement loss events is summed up, then that sum is equal to $T^* \times r$, and the data loss events could be distributed arbitrarily during this time interval. In simulating data losses, assumption 1 can be practically realized by picking W to be sufficiently large; the reasoning behind this is as follows: a larger value of W increases the number of events per unit time, and when W is sufficiently large, we can get a sufficiently large number of events over every finite time interval T^*, such that the rate of data loss is sufficiently close to r.

Analyzing closed-loop stability

In this section, we consider the closed-loop system subject to sensor data losses as defined in previous section, and analyze the stability properties (robustness) with respect to sensor data losses. Specifically, the objective is to establish, for convergence to a desired neighborhood of the origin, a data loss rate r^*, defined over a finite time interval T, such that if $r \leq r^*$ then convergence to a desired neighborhood is achieved in the presence of data losses. Note that implicit in this analysis (also in the formulation of Eq. 1) is the understanding that during the time that sensor measurements are unavailable, the values of the measured variables (in computing the control action) are "frozen" at the last available measurement. This results in the value of the manipulated variable being frozen at the last computed value. The implications of this intuitive assumption on the stabilizing properties under a given control configuration is discussed in Remark 5.

We first consider the closed-loop system under the controller of Eq. 3, where the control action is computed in an implement and hold fashion with a hold time Δ. We establish that for convergence to a desired neighborhood of the origin, there exists a bound on the implement and hold time Δ*, such that if the hold time is less than Δ*, then during the entire hold time, we get (outside of the desired neighborhood of the origin) that $\dot{V} < 0$ (by virtue of the fact that the control action is "held" at the value computed using the last available measurement) and eventual convergence to the desired neighborhood can be achieved. This analysis reveals that anytime the control action is "updated" by using the current state value, the closed-loop Lyapunov-function decreases during the next Δ (for $\Delta \leq \Delta^*$) time. In essence, it reveals that the worst distribution of the measurement loss events, or the most destabilizing that they can be, would be if they were to occur consecutively. The sum of the duration of all the measurement loss events not being greater than $r \times T^*$ over a finite time interval T^* can be exploited to yield the desired result, which is formalized in Theorem 3 below.

Theorem 3: *Consider the constrained system of Eq. 1 under the bounded control law of Eqs. 2–4 designed using the Lyapunov function V and* $\rho > 0$*, and the stability region estimate* Ω *under continuous implementation. Then, given any positive real number d such that* $\|x\| \leq d$ *implies* $x \in \Omega$ *and T* over which a data loss rate r is defined, there exists a positive real number r* such that if* $x(0) := x_0 \in \Omega$ *and is known, and* $r \in (0, r^*]$*, then* $x(t) \in \Omega \ \forall \ t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d$.

Proof of Theorem 3: The proof consists of two parts. In the first part, we assume that the measurement loss events occur consecutively, and show the existence of a bound on the data loss rate r^* below which convergence to the desired neighborhood is achieved. In part 2, we show that this result also holds for any distribution of the open loop events over the time interval T^*.

Part 1: Substituting the control law of Eqs. 2–4 into the system of Eq. 1 it can be shown that

$$\dot{V}(x) \leq -\rho^* V(x) \tag{7}$$

for all $x \in \Omega$, where Ω was defined in Eq. 4. Note that since $V(\cdot)$ is a continuous function of the state, one can find a finite, positive real number, δ', such that $V(x) \leq \delta'$ implies $\|x\| \leq d$. Consider now evolution of the states between the time 0 to T^*, where T^* is the time interval over which the data loss rate is defined, and for a given data loss rate r, denote the duration of open-loop operation as Δ. In the rest of the proof, we show the existence of a positive real number Δ* such that all state trajectories originating in Ω converge to the level set of V ($V(x) \leq \delta'$) for any value of $\Delta \in (0, \Delta^*]$. Hence, we have that $\limsup_{t\to\infty} \|x(t)\| \leq d$. We then use the definition of the data loss rate to come up with an r^* to show that the result holds for any $r \leq r^*$.

To this end, consider a "ring" close to the boundary of the stability region, described by $\mathscr{M} := \{x \in \mathrm{IR}^n : (c^{max} - \delta) \leq V(x) \leq c^{max}\}$, for a $0 \leq \delta \leq c^{max}$. Let the control action be computed for some $x(0) := x_0 \in \mathscr{M}$, and, upon unavailability of subsequent measurements, held constant until a time Δ**, where Δ** is a positive real number ($u(t) = u(x_0) := u_0 \ \forall \ t \in [0, \Delta^{**}]$) to be determined. Then, $\forall \ t \in [0, \Delta^{**}]$

$$\begin{aligned}\dot{V}(x(t)) &= L_f V(x(t)) + L_G V(x(t)) u_0 \\ &= L_f V(x_0) + L_G V(x_0) u_0 + (L_f V(x(t)) - L_f V(x_0)) \\ &\qquad + (L_G V(x(t)) u_0 - L_G V(x_0) u_0)\end{aligned} \tag{8}$$

Since the control action is computed based on the states in $\mathscr{M} \subseteq \Omega$, $L_f V(x_0) + L_G V(x_0) u_0 \leq -\rho^* V(x_0)$. By definition, for all $x_0 \in \mathscr{M}$, $V(x_0) \geq c^{max} - \delta$, therefore, $L_f V(x_0) + L_G V(x_0) u_0 \leq -\rho^*(c^{max} - \delta)$.

Since the function $f(\cdot)$, and the elements of the matrix $G(\cdot)$ are continuous, $\|u\| \leq u^{max}$, $\mathscr{M}$ is bounded, and $L_f V(\cdot)$, $L_G V(\cdot)$ are Lipschitz, then one can find, for all $x_0 \in \mathscr{M}$, positive real numbers Δ**, K^1, K^2 and K^3 such that $\|x(\tau) - x_0\| \leq K^1 \Delta^{**}$ for all $\tau \leq \Delta^{**}$, $\|L_f V(x(\tau)) - L_f V(x_0)\| \leq K^3 K^1 \Delta^{**}$, $\|L_G V(x(\tau)) u_0 - L_G V(x_0) u_0\| \leq K^2 K^1 \Delta^{**}$ for all $\tau \leq \Delta^{**}$, and $\Delta^{**} < \frac{\rho^*(c^{max} - \delta) - \varepsilon}{(K^1 K^2 + K^1 K^3)}$ where ε is a positive real number such that

$$\varepsilon < \rho^*(c^{max} - \delta) \tag{9}$$

Using these inequalities in Eq. 8, we get

$$\dot{V}(x(\tau)) \leq -\varepsilon < 0 \ \forall \ 0 \leq \tau \leq \Delta^{**} \tag{10}$$

This implies that, given δ', if we pick δ such that $c^{max} - \delta < \delta'$, then if the control action is computed for any $x \in \mathscr{M}$, and the measurement loss time is less than Δ**, we get that $\dot{V}$ remains negative during this time, and, therefore, the state of the closed-loop system cannot escape Ω (since Ω is a level set of V). We now show the existence of Δ' such that for all $x_0 \in \Omega^f := \{x \in \mathrm{IR}^n : V(x_0) \leq c^{max} - \delta\}$, we have that $x(\Delta) \in \Omega^u := \{x_0 \in \mathrm{IR}^n : V(x_0) \leq \delta'\}$, where $\delta' < c^{max}$, for any $\Delta \in (0, \Delta']$.

Consider Δ' such that

$$\delta' = \max_{V(x_0) \leq c^{max} - \delta, u \in \mathcal{U}, t \in [0, \Delta']} V(x(t)) \tag{11}$$

Since V is a continuous function of x, and x evolves continuously in time, then for any value of $\delta < c^{max}$, one can choose a sufficiently small Δ', such that Eq. 11 holds. Let $\Delta^* = \min\{\Delta^{**}, \Delta'\}$. We now show that for all $x_0 \in \Omega^u$, and $\Delta \in (0, \Delta^*]$, $x(t) \in \Omega^u$ for all $t \geq 0$.

For all $x_0 \in \Omega^u \cap \Omega^f$, by definition $x(t) \in \Omega^u$ for $0 \leq t \leq \Delta$ (since $\Delta \leq \Delta'$). For all $x_0 \in \Omega^u \backslash \Omega^f$ (and therefore $x_0 \in \mathscr{M}$), $\dot{V} < 0$ for $0 \leq t \leq \Delta$ (since $\Delta \leq \Delta^{**}$). Since Ω^u is a level set of V, then $x(t) \in \Omega^u$ for $0 \leq t \leq \Delta$.

We note that for x such that $x \in \Omega \backslash \Omega^u$, negative definiteness of $\dot{V}$ is guaranteed for $\Delta \leq \Delta^* \leq \Delta^{**}$. Finally, for all $\Delta^* \leq t \leq T^*$, negative definiteness of $\dot{V}$ is guaranteed by the control law of Eq. 3. Now for a given value of T^*, the worst case scenario (that is, the maximum time over which the system may run open-loop) involves loss of measurements for the last Δ time for a given interval, followed by consecutive loss of measurements for the first Δ time of the next interval. Therefore, continued negative definiteness of $\dot{V}$ (and convergence to the desired neighborhood) can be guaranteed if the measurement loss time in each interval Δ is less than equal to $\frac{\Delta^*}{2}$. An $r^* = \frac{\Delta^*}{2T^*}$ will ensure that the maximum duration of measurement loss over the interval T^* is less than $\Delta^*/2$, and also maximum loss of measurement between two successive intervals is less than Δ^* (If $\frac{\Delta^*}{2} > T^*$, then we have to restrict r^* to 1 to ensure that $r < 1$, and that we get at least one measurement over the entire interval T^*). Therefore, for all $x(0) \in \Omega$, there exists an r^* such that if $r \leq r^*$, $\limsup_{t\to\infty} V(x(t)) \leq \delta'$. Finally, since $V(x) \leq \delta'$ implies $\|x\| \leq d$, therefore, we have that $\limsup_{t\to\infty} \|x(t)\| \leq d$.

Part 2: Consider now the finite time interval T^*, such that for convergence to a desired neighborhood of the origin, the bound on the data loss rate r^*, under the assumption that the data-loss events all occur consecutively, has been computed. Consider now that the data-loss events do not occur continuously, but occur in N intervals, each of duration Δ_i with $\sum_{i=1}^{N} \Delta_i = T^* \times r^*$. From part 1 of the proof, for each of these durations Δ_i, negative definiteness of $\dot{V}$ can be established. For the duration during which the measurements are available, $\dot{V} < 0$ is achieved by virtue of the control law. In summary, having established the bound r^* under consecutive loss of measurement, the same bound r^* continues to guarantee practical stability irrespective of the distribution of the measurement loss events. This completes the proof of Theorem 3.

Remark 4: Note that one can easily remove the assumption that x_0 is known by "stepping back" from the boundary of the stability region enough to ensure that during the time r^*T^*, the state trajectory cannot escape the boundary of the stability region. By the definition of rate of data loss, the first measurement is guaranteed to be available by $(r^*T^*)^+$. Any time during the interval T^* that a measurement is received with the state still residing in the stability region (due to the "stepping back") Theorem 3 can be used to establish practical stability. Note also, that the value of r^* depends on the interval T^* over which it is defined (see the simulation example in section for a demonstration). To understand this more clearly, let us revisit the proof of Theorem 3. It can be seen that for convergence to a desired neighborhood of the origin, one can come up with a value Δ^*, such that if only one measurement was received every Δ^*, then convergence to the desired neighborhood would be achieved. Theorem 3 exploits this fact together with the definition of the data loss rate, to ensure that over a Δ^* duration within T^* (and across two time intervals), at least one measurement is received. In summary, Δ^* is fixed by the given size of the neighborhood to the origin where convergence is desired (δ'); given a T^* over which the data loss rate is defined, r^* can then in turn be picked such that the maximum duration of open-loop behavior across intervals stays less than Δ^*.

Remark 5: In our results, no bound on the open-loop instability is assumed to be known, leading to practical (and not asymptotic) stability to the desired equilibrium point. If additional assumptions are made on the open-loop growth of the Lyapunov-function (locally) around the desired equilibrium point, asymptotic stability can be shown using the same line of reasoning as in.[48] Specifically, during the time that the measurements are not available, the value of V is allowed to increase during T^*, so long as the increase in V can be "countered" by the decrease in V during the rest of the time (which relies on assuming a known measure of open-loop instability). The limitations imposed by the presence of constraints, however, would still need to be accounted for, with the data loss rate having to be defined over a finite interval. Furthermore, the set of stabilizable initial conditions will only be a subset of Ω, such that starting from this subset, the closed-loop state can not escape Ω during the time of open-loop evolution r^*T^*. In our results, with x_0 known, r^* is picked so that $\dot{V}$ stays negative during the entire duration of T^* (until convergence to the desired neighborhood is achieved), thereby, obviating the need to restrict the set of initial conditions to a subset of Ω. Note also that V being allowed to increase during T^* (as long as it decays by the end of T^*) could possibly lead to a larger allowable r^*. The tradeoff would be that the Lyapunov function would not be guaranteed to decay all the time but only to decay in value at steps of T^*, and it could take longer to reach the desired neighborhood of the origin. Note that the problem considered in this work is not that of ascertaining finite-time stability (ensuring convergence to the desired equilibrium point in finite time, see, for example,[31]) under continuous availability of measurement, but rather that of analyzing preservation of stability under asynchronous measurements. Note that for the case when sensor measurements are lost but it is possible to change the value of the manipulated input, statistical (for example,[32]) or first principles model based methods designed to "fill-in" the unavailable state measurement can very well be included within the proposed framework, and can serve to improve the data-loss handling capabilities of the control designs (depending upon the accuracy of the data prediction). The proposed fault-tolerant control structure, however, addresses a more general problem, that of intermittent loss of communication between the controller and the process, including asynchronous measurements, as well as the inability to change the manipulated input value during the communication lapses.

Remark 6: The proof of theorem 3 relies on the stabilizing properties of the controller during the time that measurements are not available to ensure that even during that time $\dot{V} < 0$. Note that the rate of decay of the Lyapunov function that is achieved under continuous measurements is closely related to how much data loss can be tolerated in the system in the sense that for a given process, and constraints on the manipulated inputs, if one control law achieves greater decay of the Lyapunov function over the other, then it can tolerate greater sensor data loss compared to the other (note that the tradeoff could be a smaller stability region estimate). The continued decay of the Lyapunov function, however, can only be achieved over a finite time, and in turn, requires the data loss rate to be defined over a finite time. Even if one were to use the approach discussed in Remark 4 to come up with an alternate bound, the limitations imposed by the constraints on the definition of the rate of data loss (specifically, the need to define it over a finite time interval) would be present and can be understood as follows: If there were no constraints, $\dot{V} < 0$ under continuous measurement could possibly be achieved over the entire state space. No matter how "far" the states go during the unavailability of measurements, when (over the infinite time duration) the measurements do become available, one could require them to be available for a large enough time (compared to the time for which they were not available) to achieve an overall reduction in the value of the Lyapunov function. Constraints, how-

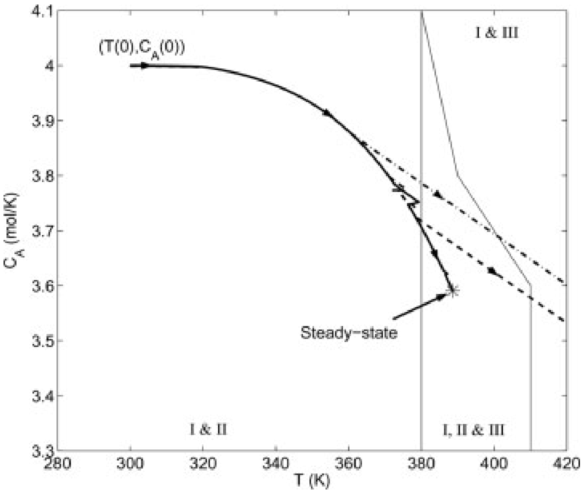

Figure 4. Evolution of the state trajectory under control configuration 2 in the presence of sensor data loss (defined over a finite interval) at a rate of 0.4 (dashed line), sensor data loss (defined over an infinite interval) at a rate of 0.05 (dash-dotted line), and sensor data loss (defined over a finite interval) at a rate of 0.1 (solid line).

ever, limit the set of initial conditions (estimated using the stability region Ω) starting from where $\dot{V} < 0$ is achievable. If the measurements are not available for a large duration, the states may go too "far" (that is, out of the stability region) and then even if measurements were available for all time after that, $\dot{V} < 0$ could not be achieved simply due to limited available control action (see the simulation example for a demonstration). In contrast, defining the data loss rate over a finite time interval enables restricting the states to stay within the region from where $\dot{V} < 0$, and, hence, closed-loop stability is achievable.

Remark 7: Note that the specific problem that this work considers yields a solution that is essentially different from, and cannot be handled by simply using adaptive or other robust control approaches. These approaches, however, can very well be integrated within the proposed framework. The key requirement being that the controller design (whether it be an adaptive control design or another robust controller design) for the individual control configuration allow for an explicit characterization of its stability properties in the presence of input constraints and asynchronous data losses. It is this characterization that can be subsequently used in fault-tolerant reconfiguration strategies. Note also that multirate data loss problems, where data is available at predetermined (but different) times for the different measurements can be analyzed as special cases for the problem considered in the present work which does not assume data availability at predetermined rates.

Control of a chemical reactor subject to sensor data loss

Consider the chemical reactor of Eq. 5 again with the inlet stream temperature, as the manipulated input $u_2 = T_{A0} - T_{A0s}$, subject to the constraints $|u_2| \leq u_{max}^2 = 100$ K, and subject to measurement data losses. We first design the bounded controller and estimate the stability region (see Figure 4). For a given value of $T^* = 10$ min, we pick a value of $W = 10$ events per minute (the simulations are run as discussed in section); which yields an overall event rate of $1/W$ that is, about one event every six seconds (or about 100 events in 10 min). It was verified that with this value of W, the rate of data loss, as defined, was approximately achieved over the duration of every ten minutes, in other words, that $W = 10$ is a sufficiently large value of W. Starting from an initial condition within the stability region of the first configuration, the closed-loop system is unstable with a data loss rate $r = 0.4$ (dashed lines in Figure 4; the corresponding manipulate input profile can be seen in Figure 5). However, if the data loss rate is kept at 0.1, closed-loop stability is achieved (see solid lines in Figures. 4–5), demonstrating the need for the data loss to be sufficiently small.

The next simulation run demonstrates the dependence of r^* on the time interval over which it is defined (as discussed in Remark 6). Specifically, we now run the same simulation with an even smaller data loss rate ($r = 0.05$), however, with the data rate defined over the duration of the simulation of 68 min. A scenario where measurements are received continuously for the first five minutes, lost consecutively for the next 3.6 min, and received thereafter results in an overall rate of data loss of only 0.05. We see however, that closed-loop stability is not achieved (dash-dotted lines in Figures 4–5). This is so because with this larger value of T^*, the acceptable bound on the rate of data loss decreases, and illustrates the interconnection between the maximum allowable data loss rate, and the interval over which it is defined. In summary, the above simulations demonstrate the need for the data loss rate to be less than what the system can tolerate

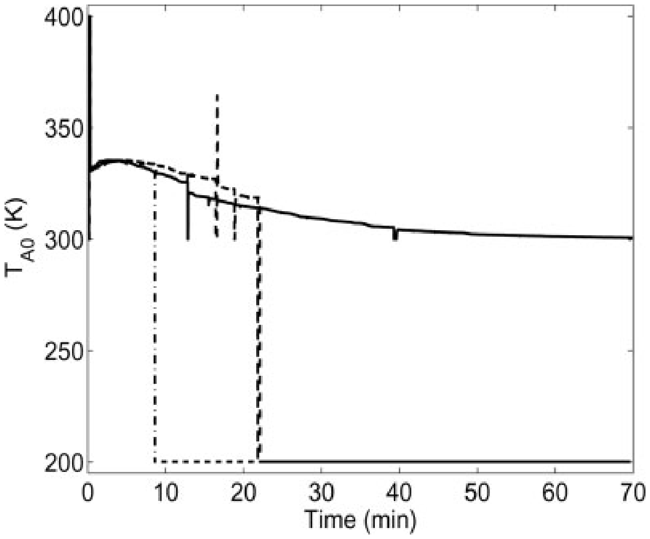

Figure 5. Manipulated input profile under control configuration 2 in the presence of sensor data loss (defined over a finite interval) at a rate of 0.4 (dashed line), sensor data loss (defined over an infinite interval) at a rate of 0.05 (dash-dotted line), and sensor data loss (defined over a finite interval) at a rate of 0.1 (solid line).

(that is, for $r \leq r^*$), with r^* appropriately computed for a given time interval T^* over which the rate is defined.

Fault-Tolerant Control Subject to Sensor Data Losses

Having analyzed the stability properties of the individual control configurations subject to sensor data losses, in this section we present a fault-tolerant controller that maintains closed-loop stability in the presence of sensor data losses.

Reconfiguration law

Fault-tolerance is achieved via switching to a backup configuration for which the state of the closed-loop system is within the stability region, and the sensor data loss rate is less than the bound on the data loss rate required for closed-loop stability. To formalize this idea, consider the constrained nonlinear system of Eq. 1 for which the bounded controllers of the form of Eq. 3 have been designed and the stability regions Ω_j, $j = 1, \ldots, N$ have been explicitly characterized under each control configuration, and the bounds on the data loss rate r_j^*, $j = 1, \ldots, N$ for a given interval T have been computed. Let $d_{max} = \max_{j=1,\ldots,N} d_j$, where d_j was defined in Theorem 3 and let $\Omega_U = \bigcup_{j=1}^{N} \Omega_j$. We consider the problem where the process starts operating under configuration i with a data loss rate of $r_i(0)$, and at some point in time the data-loss rate $r(t)$ possibly becomes greater than r_i^*.

Theorem 4: *Let $k(0) = i$ for some $i \in \mathscr{K}$ and $x(0) := x_0 \in \Omega_i$. Let T^f be the earliest time such that $r(t) > r_i^*$ with $x(T^f)$ measured. Then, the following switching rule*

$$k(t) = \left\{ \begin{array}{ll} i, & 0 \leq t < T^f \\ l, & t \geq T^f, x(T^f) \in \Omega_l, r(T^f) \leq r_1^* \end{array} \right\} \tag{12}$$

and $r(t) \leq r_l^*$ $\forall$ $t \geq T^f$ guarantees that $x(t) \in \Omega_U$ $\forall$ $t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d_{max}$.

Proof of Theorem 4: We consider the two possible cases; first if the data-loss rate r stays less than or equal to r_i^* for all times, and second if $r > r_i^*$ at some time T^f.

Case 1: The absence of a switch implies $k(t) = i$ $\forall$ $t \geq 0$. Furthermore, since $x(0) \in \Omega_i$, $r(t) \leq r_i^*$ and control configuration i is implemented for all times in this case, we have that $x(t) \in \Omega_i$ $\forall$ $t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d_i$. Finally, since $\Omega_i \subseteq \Omega_U$ and $d_i \leq d_{max}$, we have that $x(t) \in \Omega_U$ $\forall$ $t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d_{max}$.

Case 2: At time T^f, the supervisor switches to a control configuration l for which $x(T^f) \in \Omega_l$ and $r \leq r_l^*$. From this time onwards, since configuration l is implemented in the closed-loop system for all times, and since $x(T^f) \in \Omega_l$ and $r(t) \leq r_l^*$, we have that $x(t) \in \Omega_l$ $\forall$ $t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d_l$. As in case 1, since $\Omega_l \subseteq \Omega_U$ and $d_l \leq d_{max}$, we have that $x(t) \in \Omega_U$ $\forall$ $t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d_{max}$. This completes the proof of Theorem 4.

Remark 8: Theorem 4 explicitly takes into consideration the constraints in the manipulated inputs, and the measurement losses in deciding which backup configuration to implement in the closed-loop system, and, therefore, requires that a backup configuration is implemented for which the state resides in its stability region *and* the data loss rate is less than the data loss rate that the backup configuration can tolerate. Disregarding either of these factors could lead to instability (see the simulation example for a demonstration).

Remark 9: Note that the result of Theorem 4 assumes explicit knowledge of the current data loss rate to not only identify the appropriate backup configuration, but also to trigger reconfiguration. In this sense, the reconfiguration logic has an in-built fault detection mechanism, with faults being defined as data loss rate exceeding the allowable data loss rate. In practice, the data loss rate can only be estimated over finite intervals of time, and this estimate can be used in deciding which backup configuration should be activated according the reconfiguration rule of Theorem 4. Note also, that other than the data loss rate (estimate) going over the allowable bound, other means of detecting instability like behavior (such as the state trajectory going close to the boundary of the stability region under the currently-active control configuration), can be used to trigger the reconfiguration. It is worth pointing out, however, that this fault-detection capability is only limited to the rate of data loss exceeding the tolerable value. As discussed in Remark 3, explicit fault detection mechanisms which detect faults in the sensors (such as sensors reporting incorrect values) can be used within the proposed approach to tackle sensor faults manifested as erroneous measurements.

Remark 10: While we assume the availability of measurements of all the state variables, the same approach can be used to analyze the case where each control configuration is comprised of a set of sensors and actuators with the sensors (measurements) different in different control configurations. Specifically, under each control configuration, an estimation scheme, coupled with the feedback controller, will have to be implemented, and the output feedback-stability region, subject to constraints and sensor data losses characterized. Subsequently, the reconfiguration rule will have to be modified to account for the fact that the reconfiguration decision is made on the basis of state estimates (which may contain errors); for a switching scheme that addresses these issues in the context of switched nonlinear systems under continuous output feedback control, see.[36]

Fault-tolerant control of a chemical reactor

Consider, once again, the chemical reactor of Eq. 5 in the presence of sensor data losses. As seen in Figure 5, the closed-loop system using configuration 2 experiences instability when the data loss rate becomes 0.4. In the event of such data losses, one of the backup control configurations need to be activated, and this choice cannot be made only by looking at the states with respect to the stability region. In this section, we demonstrate the application of the switching rule of Theorem 4 that achieves fault-tolerance. To this end, we first characterize the stability region under each backup configuration. Figure 6 depicts the stability region, in the (T, C_A) space, for each configuration. The desired steady-state is depicted with an asterisk that lies in the intersection of the three stability regions. For configurations 1, 2 and 3, the bound on the data loss rate is estimated at $r_1^* = 0.35$, $r_2^* = 0.3$ and $r_3^* = 0.15$, respectively.

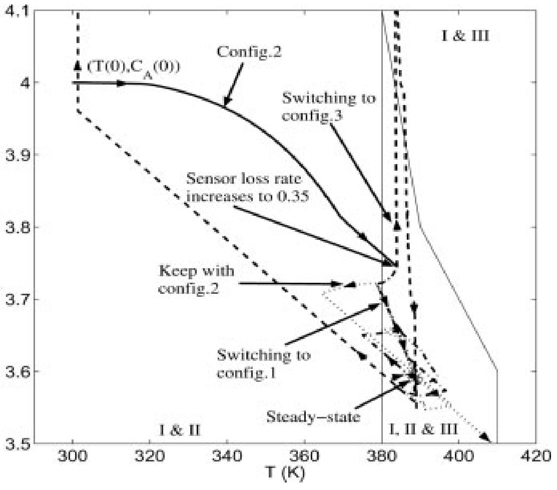

Figure 6. Evolution of the state trajectory: At t = 13.5 min the data loss rate goes up to 0.35 under configuration 2 (solid line).

Keeping with configuration 2 (dotted line) or switching to configuration 3 (dashed line) does not preserve stability, while switching to configuration 1 (dash-dotted line) preserves stability.

We consider an initial condition, $T(0) = 300\ K$, $C_A(0) = 4.0$ mol/L, $C_B\ (0) = 0.0$ mol/L, using the T_{A0}-control configuration within the stability region of configuration 2, and consider a case where the rate of sensor data loss increases from an initial value of 0.1 to 0.35. As shown by the solid line in Figure 6, the controller proceeds to drive the closed-loop trajectory towards the desired steady-state, up until time 13.5 min of reactor startup when the sensor data-loss rate increases to 0.35. If the supervisor does not use the result of Theorem 4 to trigger reconfiguration, but persists with using configuration 2, stability is not achieved (see dotted lines in Figures 6–7). Note that at this time, the state of the closed-loop system resides in the stability region of both backup configurations 1 and 3. If the supervisor does implement reconfiguration, but in a way that does not account for the presence of sensor data loss and activates configuration 3, the state trajectory does not converge to the desired steady-state (see dashed line in Figure 6) even though the state at the switching time is within stability region of control configuration 3. This happens because the rate of data loss is not within the tolerable bound for configuration 3. In contrast, if the reconfiguration rule of Eq. 12 is implemented, and the supervisor activates configuration 1, the state trajectory converges to the desired steady-state (see dashed-dotted line in Figure 6). The corresponding manipulated input profiles are shown in Figure 7.

Fault-tolerant control of a polyethylene reactor subject to sensor data loss

Having demonstrated the application of the proposed fault-tolerant controller on the illustrative example, we next consider a more complex process, specifically, an industrial gas-phase polyethylene reactor system (see Figure 8). This reactor was also studied in[39] in the context of faults in the control actuator (under assumption of continuous availability of process measurements).

The feed to the reactor consists of ethylene, comonomer, hydrogen, inerts, and catalyst. A stream of unreacted gases flows from the top of the reactor and is cooled by passing through a heat exchanger in counter-current flow with cooling water. Cooling rates in the heat exchanger are adjusted by instantaneously blending cold and warm water streams, while maintaining a constant total cooling water flow rate through the heat exchanger. Mass balance on hydrogen and comonomer have not been considered in this study because hydrogen, and comonomer have only mild effects on the reactor dynamics.[35] A mathematical model for this reactor has the form:[34]

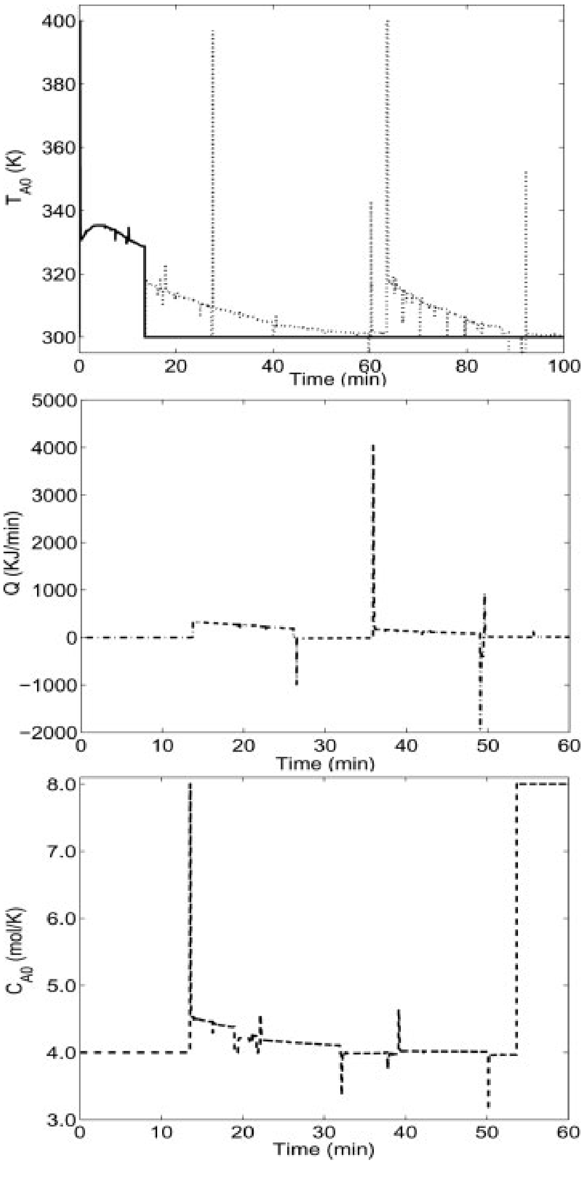

Figure 7. Manipulate input profiles: At t = 13.5 minutes the data loss rate goes up to 0.35 under configuration 2 (solid line), switching to configuration 3 does not preserve stability (dashed line), while switching to configuration 1 (dash-dotted line) preserves stability.

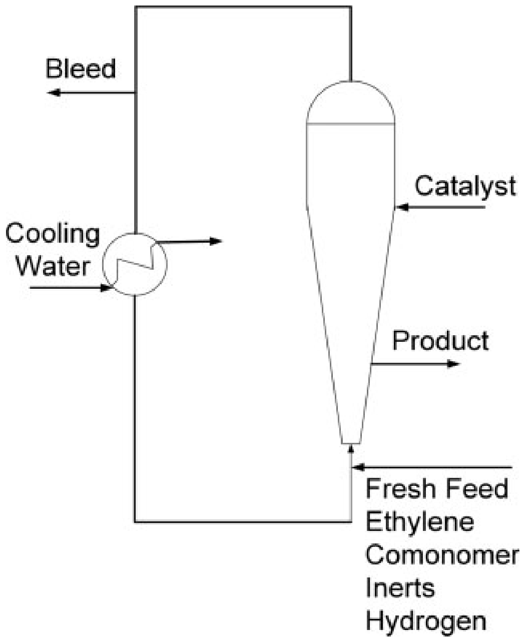

Figure 8. Industrial gas-phase polyethylene-reactor system.

$$
\begin{aligned}
\frac{d[In]}{dt} &= \frac{F_{In} - \dfrac{[In]}{[M_1]+[In]} b_t}{V_g}\\
\frac{d[M_1]}{dt} &= \frac{F_{M_1} - \frac{[M_1]}{[M_1]+[In]} b_t - R_{M1}}{V_g}\\
\frac{dY_1}{dt} &= F_c a_c - k_{d_1} Y_1 - \frac{R_{M1} M_{W_1} Y_1}{B_w}\\
\frac{dY_2}{dt} &= F_c a_c - k_{d_2} Y_2 - \frac{R_{M1} M_{W_1} Y_2}{B_w}\\
\frac{dT}{dt} &= \frac{H_f + H_{g1} - H_{g0} - H_r - H_{pol}}{M_r C_{pr} + B_w C_{ppol}}\\
\frac{dT_{w_1}}{dt} &= \frac{F_w}{M_w}(T_{wi} - T_{w_1}) - \frac{UA}{M_w C_{pw}}(T_{w_1} - T_{g_1})\\
\frac{dT_{g_1}}{dt} &= \frac{F_g}{M_g}(T - T_{g_1}) + \frac{UA}{M_g C_{pg}}(T_{w_1} - T_{g_1}) \qquad (13)
\end{aligned}
$$

where

$$
\begin{aligned}
b_t &= V_p C_v \sqrt{([M_1]+[In]) \cdot RR \cdot T - P_v}\\
R_{M1} &= [M_1] \cdot k_{p0} \cdot exp\left[\frac{-E_a}{R}\left(\frac{1}{T} - \frac{1}{T_f}\right)\right] \cdot (Y_1 + Y_2)\\
C_{pg} &= \frac{[M_1]}{[M_1]+[In]} C_{pm1} + \frac{[In]}{[M_1]+[In]} C_{pIn}\\
H_f &= F_{M_1} C_{pm1}(T_{feed} - T_f) + F_{In} C_{pIn}(T_{feed} - T_f)\\
H_{g1} &= F_g (T_{g1} - T_f) C_{pg}\\
H_{g0} &= (F_g + b_t)(T - T_f) C_{pg}\\
H_r &= H_{reac} M_{W_1} R_{M1}\\
H_{pol} &= C_{ppol}(T - T_f) R_{M1} M_{W_1} \qquad (14)
\end{aligned}
$$

For the definition of all the variables used in Eqs. 13–14, the values of the process parameters, and details on controller design, see.[39] The open-loop system at the nominal operating condition exhibits an unstable equilibrium point surrounded by a limit cycle. The control objective is to stabilize the reactor at the unstable equilibrium point using measurements of the state variables. To accomplish this objective we consider the following manipulated input candidates:

1. Catalyst flow rate, $u_1 = (F_c - F_c^{\,s})a_c$, subject to the constraint $|u_1| \leq u^1_{max} = (\frac{2}{3600})a_c \frac{mol}{s}$.
2. Feed temperature, $u_2 = \frac{F_{M_1}C_{pm1} + F_{In}C_{pIn}}{M_r C_{pr} + B_w C_{ppol}}(T_{feed} - T^s_{feed})$, subject to the constraint $|u_2| \leq u^2_{max} = \frac{F_{M_1}C_{pm1} + F_{In}C_{pIn}}{M_r C_{pr} + B_w C_{ppol}}(20)\frac{K}{s}$.

First, process operation under primary control configuration was considered (that is, the catalyst flow rate, F_c, was the manipulated input) and a bounded nonlinear controller was designed using the formula of Eqs. 2–4. Specifically, a quadratic function of the form $V_1 = e_1^T P_1 e_1$ and $\rho_1 = 0.01$ were used to design the controller, and a composite Lyapunov function of the form $V_{c_1} = 5 \times 10^{-3}\ (In - In_s)^4 + 5 \times 10^{-4}(M_1 - M_{1s})^2 + 5 \times 10^{-11}(Y_1 - Y_{1s})^2 + 5 \times 10^{-11}(Y_2 - Y_{2s})^2 + 5 \times 10^{-4}(T - T_s)^2 + 5 \times 10^{-11}(T_{w_1} - T_{w_{1s}})^2 + 5 \times 10^{-11}(T_{g_1} - T_{g_{1s}})^2$ was used to estimate the stability region of the primary control configuration yielding a $c_1^{max} = 56.8$. A quadratic Lyapunov function of the form $V_2 = \frac{1}{2}(T - T_s)^2$ and $\rho_2 = 0.01$ were used to design the controller that used

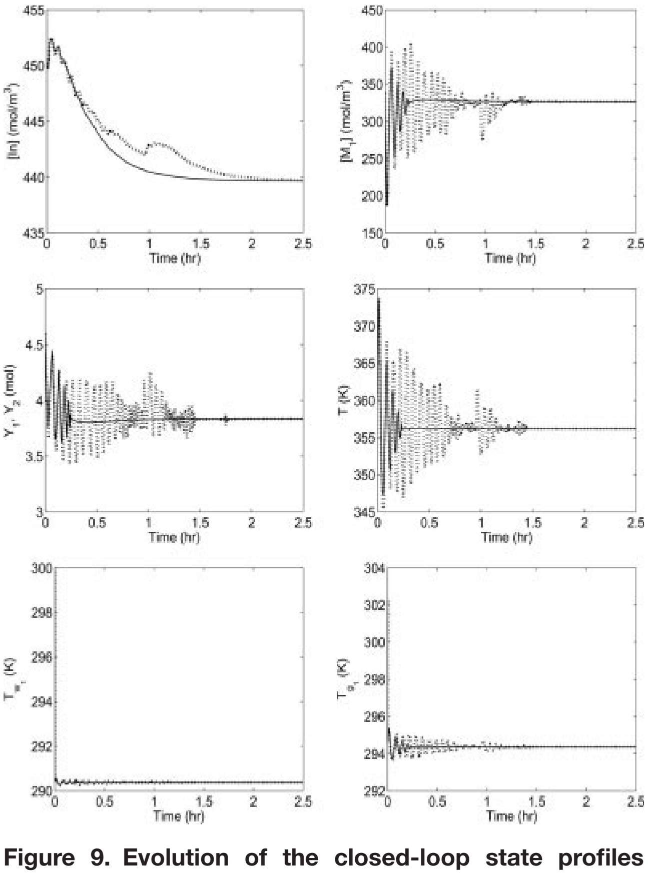

Figure 9. Evolution of the closed-loop state profiles under primary control configuration under continuous measurements (solid lines), and sensor data loss rate of 0.75 (dotted lines).

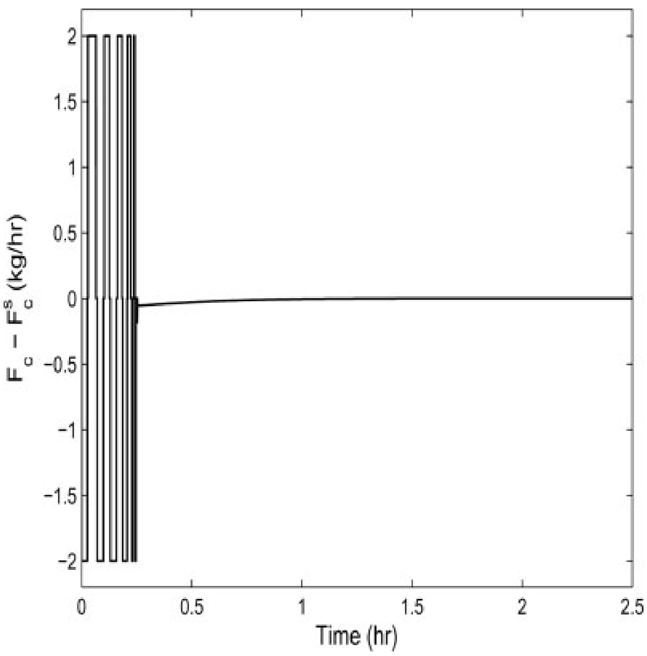

Figure 10. Evolution of the manipulated input profile under primary control configuration under continuous measurements.

the fall-back control configuration (that is, the feed temperature T_{feed}, was the manipulated input), and a composite Lyapunov function of the form $V_{c_2} = 5 \times 10^{-3}(In - In_s)^4 + 5 \times 10^{-4}(M_1 - M_{1s})^2 + 5 \times 10^{-11}(Y_1 - Y_{1s})^2 + 5 \times 10^{-11}(Y_2 - Y_{2s})^2 + 5 \times 10^{-4}(T - T_s)^2 + 5 \times 10^{-2}(T_{w_1} - T_{w_{1s}})^2 + 5 \times 10^{-11}(T_{g_1} - T_{g_{1s}})^2$ was used to estimate the stability region of the fallback control configuration yielding a $c_2^{max} = 62$.

Figure 9 shows the evolution of the closed-loop state profiles under continuous measurement (solid lines) starting from the initial condition $In(0) = 450\ \frac{mol}{m^3}$, $M_1(0) = 340\ \frac{mol}{m^3}$, $Y_1(0) = 4.6\ mol$, $Y_2(0) = 4.6\ mol$, $T(0) = 360\ K$, $T_{w_1}(0) = 300\ K$, and $T_{g_1}(0) = 300\ K$ for which $V_{c_1} = 56.78$. Since this initial state is within the stability region of the primary control configuration (that is, $V_{c_1}(x(0)) \leq c_1^{max}$), the primary control configuration is able to stabilize the system at the steady-state of interest. The corresponding manipulated inputs are shown on Figures 10–11. The dynamics of the process also reveal an important feature regarding tolerance to sensor data losses. Specifically, for this particular process, even under no control (equivalent to complete data loss), the process goes to a limit cycle which is within the stability region for the closed-loop system under continuous availability of measurements. This characteristic impacts positively on the tolerance of the closed-loop system to data losses, and a high-sensor data-loss rate of 0.75 ends up being tolerable (see dotted lines in Figures 9 and 11), even with the value of the manipulated input variable set to the nominal value during the time that the measurements are unavailable (equivalent to open-loop operation).

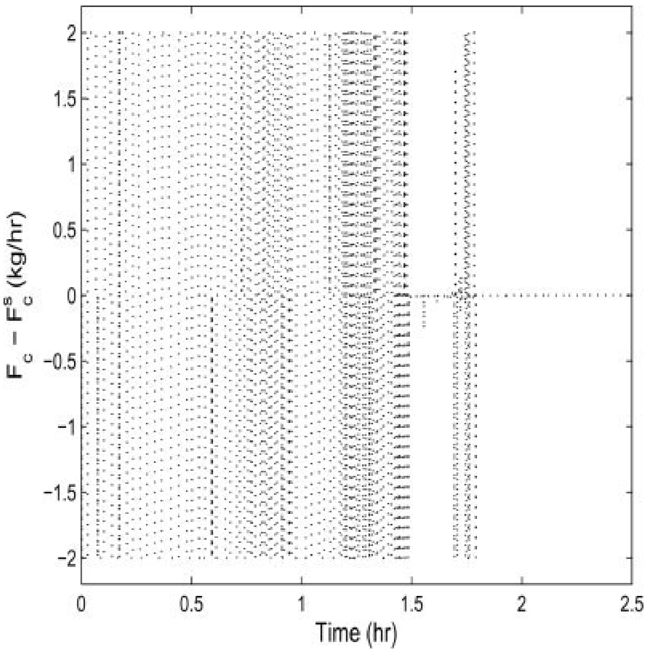

Figure 11. Evolution of the manipulated input profile under primary control configuration with sensor data loss rate of 0.75.

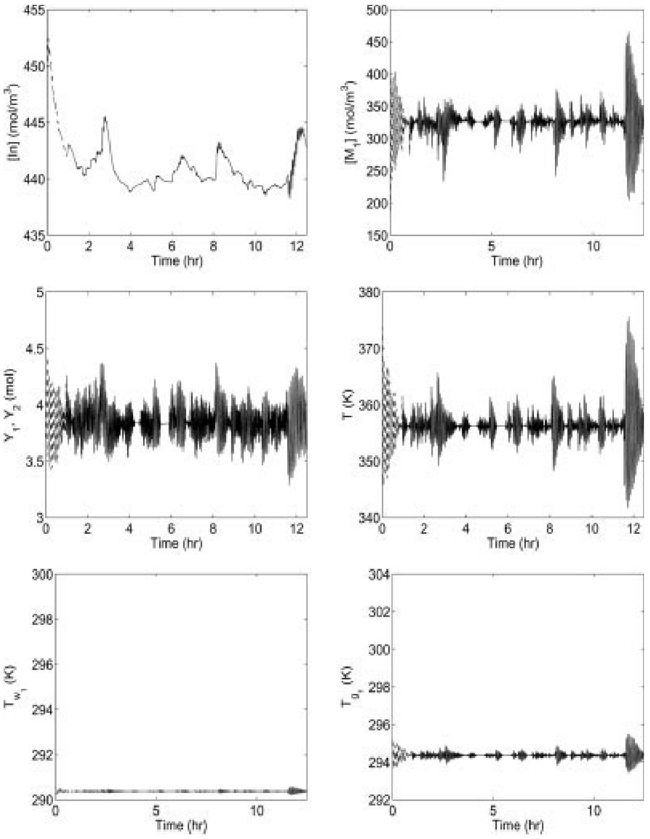

Figure 12. Evolution of the closed-loop state profiles under the primary configuration with the data loss rate increasing from 0.75 to 0.80 at 0.97 h.

Consider now a case where the rate of sensor data loss increases from an initial value of 0.75 to 0.80 at 0.97 h of reactor startup. As shown by the dashed lines in Figure 12, the controller proceeds to drive the closed-loop trajectory towards the desired steady-state up until 0.97 h. If the supervisor does not account for the increase of sensor data loss and continues utilizing the primary control configuration to control the reactor, the state trajectory does not converge to the desired steady-state (see Figure 12) even though the state at the time that the data-loss rate increases is within the stability region of the primary configuration ($V_{c_1}(x(t = 0.97\ hour)) = 1.6380 \le c_1^{max}$). This happens because the rate of data loss is not within the tolerable bound for primary control configuration ($r > r_1^* = 0.75$).

In this case, the supervisor had available a fall-back control configuration with the feed temperature as the manipulated input. At time 0.97 h when sensor data-loss rate increases from 0.75 to 0.80, $V_{c_2} = 1.6382$ implying that the state of the closed-loop system resides in the stability region of the fall-back configuration (that is, $V_{c_2}\ (x(t = 0.97\ hour)) \le c_2^{max}$), as well as $r \le r_2^* = 0.95$. If the reconfiguration rule of Eq. 12 is implemented, and the supervisor activates the fall-back configuration, the state trajectory converges to the desired steady-state (see Figure 13). The corresponding manipulated input profiles are shown in Figure 14.

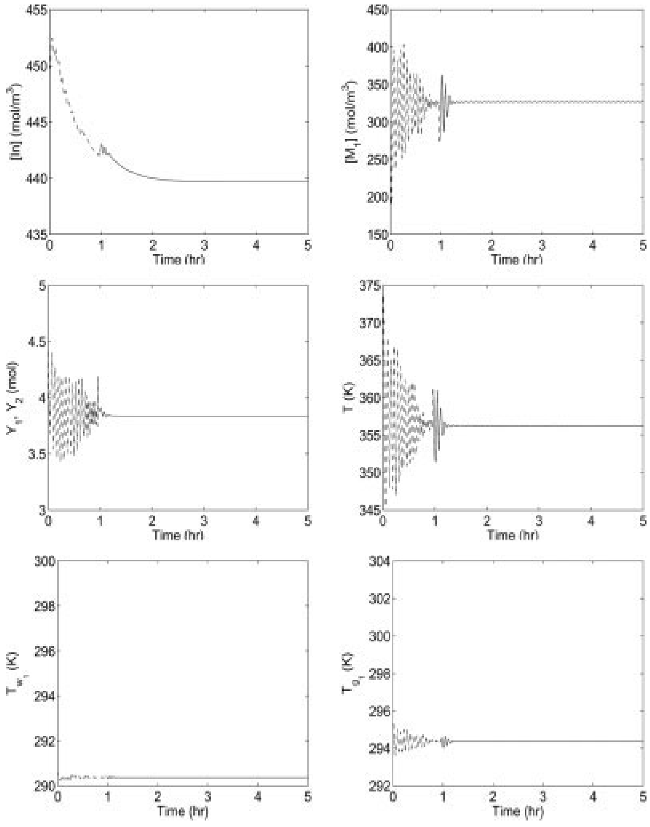

Figure 13. Evolution of the closed-loop state profiles under the reconfiguration law of Eq. 12 with the data loss rate increasing from 0.75 to 0.80 at 0.97 h.

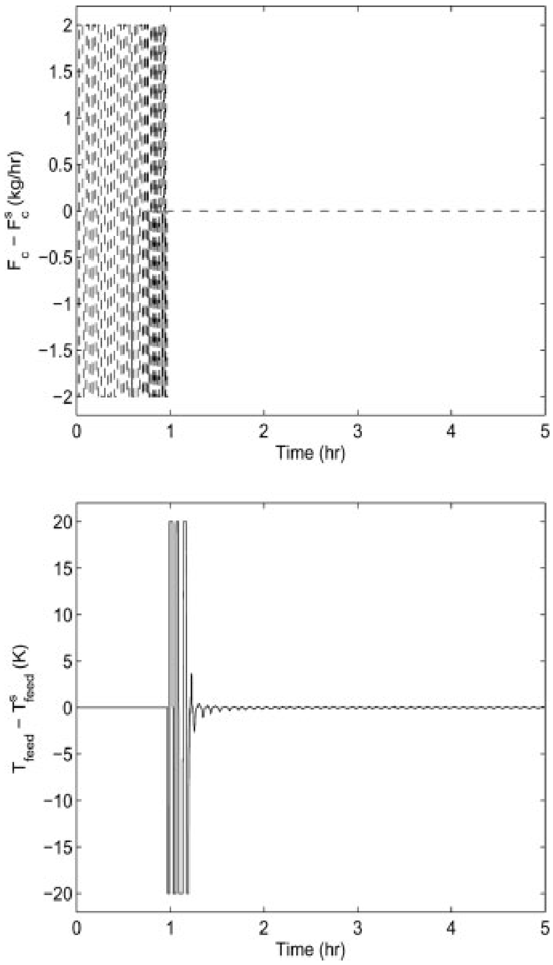

Figure 14. Evolution of the closed-loop input profiles under the reconfiguration law of Eq. 12 with the data loss rate increasing from 0.75 to 0.80 at 0.97 h.

Conclusions

In this work we considered the problem of designing a fault-tolerant controller for nonlinear process systems subject to constraints and sensor data losses. Having identified candidate control configurations for a given system, we first explicitly characterized the stability properties that is, the set of initial conditions starting from where closed-loop stabilization under continuous availability of measurements is guaranteed, as well as derived a bound on the maximum allowable data-loss rate which preserves closed-loop stability. This characterization was utilized in designing a reconfiguration logic that was shown to achieve practical stability in the presence of sensor data losses. The application of the proposed method was illustrated using a chemical process example and demonstrated on a polyethylene reactor.

Acknowledgments

Financial support from NSF, CTS-0529295, is gratefully acknowledged.

Literature Cited

1. Valluri S, Soroush M, Nikravesh M. Shortest-prediction-horizon non-linear model-predictive control. *Chem Eng Sci*. 1998;53:273–292.
2. Garcia CE, Prett DM, Morari M. Model predictive control – Theory and practice – A survey. *Automatica*. 1989;25:335–348.
3. Zhou DH, Frank PM. Fault diagnostics and fault tolerant control. *IEEE Transactions on Aerospace and Electronic Systems*. 1998;34: 420–427.
4. Bequette BW. Nonlinear predictive control using multirate sampling. *Canadian J of Chem Eng*. 1991;69:136–143.
5. Sheng J, Chen TW, Shah SL. Optimal filtering for multirate systems. *IEEE Transactions on Circuits and Systems II – Express Briefs*. 2005;52:228–232.
6. Zhang W, Branicky MS, Phillips SM. Stability of networked control systems. *IEEE Control Systems Magazine*. 2001;21:84–99.
7. Bequette BW. Nonlinear control of chemical processes – A review. *Ind & Eng Chem Res*. 1991;30:1391–1413.
8. Bao J, Zhang WZ, Lee PL. Decentralized fault-tolerant control system design for unstable processes. *Chem Eng Sci*. 2003;58:5045–5054.
9. Musulin E, Bagajewicz M, Nougues JM, Puigjaner L. Instrumentation design and upgrade for principal components analysis monitoring. *Ind & Eng Chem Res*. 2004;43:2150–2159.
10. Kapoor N, Daoutidis P. Stabilization of systems with input constraints. *Intl J of Control*. 1997;66:653–675.
11. Massoumnia M, Verghese GC, Wilsky AS. Failure detection and identification. *IEEE Transactions on Automatic Control*. 1989;34: 316–321.
12. Garcia EA, Frank PM. Deterministic nonlinear observer-based approaches to fault diagnosis: A survey. *Control Eng Practice*. 1997;5:663–670.
13. Lin Y, Sontag ED. A universal formula for stabilization with bounded controls. *Systems & Control Letts*. 1991;16:393–397.
14. Teel AR. Global stabilization and restricted tracking for multiple integrators with bounded controls. *Systems & Control Letts*. 1992;18: 165–171.
15. Rollins DK, Davis JF. Gross error-detection when variance-covariance matrices are unknown. *AIChE J*. 1993;39:1335–1341.
16. Aradhye HB, Bakshi BR, Strauss RA, Davis JF. Multiscale SPC using wavelets: Theoritical analysis and properties. *AIChE J*. 2003;49: 939–958.
17. Tatiraju S, Soroush M, Ogunnaike BA. Multirate nonlinear state estimation with application to a polymerization reactor. *AIChE J*. 1999; 45:769–780.
18. Chen JG, Bandoni JA, Romagnoli JA. Robust PCA and normal region in multivariate statistical process monitoring. *AIChE J*. 1996;42: 3563–3566.
19. Bagajewicz M, Cabrera E. A new MILP formulation for instrumentation network design and upgrade. *AIChE J*. 2002;48:2271–2282.
20. Aradhye HB, Bakshi BR, Davis JF, Ahalt SC. Clustering in wavelet domain: A multiresolution ART network for anomaly detection. *AIChE J*. 2004;50:2455–2466.
21. Yang GH, Wang JL, Soh YC. Reliable H_∞ control design for linear systems. *Automatica*. 2001;37:717–725.
22. Wu NE. Coverage in fault-tolerant control. *Automatica*. 2004;40: 537–548.
23. Mayne DQ, Rawlings JB, Rao CV, Scokaert POM. Constrained model predictive control: Stability and optimality. *Automatica*. 2000;36:789–814.
24. Kokotovic P, Arcak M. Constructive nonlinear control: A historical perspective. *Automatica*. 2001;37:637–662.
25. Harris TJ, Boudreau F, MacGregor JF. Performance assessment of multivariable feedback controllers. *Automatica*. 1996;32:1505–1518.
26. Frank PM. Fault-diagnosis in dynamic-systems using analytical and knowledge-based redundancy – A survey and some new results. *Automatica*. 1990;26:459–474.
27. Garcia-Osorio V, Ydstie BE. Distributed, asynchronous and hybrid simulation of process networks using recording controllers. *Int J of Robust & Nonlinear Control*. 2004;14:227–248.
28. Saberi A, Stoorvogel AA, Sannuti P, Niemann H. Fundamental problems in fault detection and identification. *Int J of Robust & Nonlinear Control*. 2000;10:1209–1236.
29. Niemann H, Saberi A, Stoorvogel AA, Sannuti P. Exact, almost and delayed fault detection: An observer based approach. *Int J of Robust & Nonlinear Control*. 1999;9:215–238.
30. De Persis C, Isidori A. On the design of fault detection filters with game-theoretic-optimal sensitivity. *Int J of Robust & Nonlinear Control*. 2002;12:729–747.
31. Bhat SP, Bernstein DS. Finite-time stability of continuous autonomous systems. *SIAM J on Control and Optimization*. 2000;38:751–766.
32. Nelson PRC, Taylor PA, MacGregor JF. Missing data methods in PCA and PLS: Score calculations with incomplete observations. *Chemometrics and Intelligent Laboratory Systems*. 1996;35:45–65.
33. Mehranbod N, Soroush M, Panjapornpon C. A method of sensor fault detection and identification. *J of Process Control*. 2005;15: 321–339.
34. Dadebo SA, Bell ML, McLellan PJ, McAuley KB. Temperature control of industrial gas phase polyethylene reactors. *J of Process Control*. 1997;7:83–95.
35. McAuley KB, Macdonald DA, McLellan PJ. Effects of operating conditions on stability of gas-phase polyethylene reactors. *AIChE J*. 1995;41:868–879.
36. El-Farra NH, Mhaskar P, Christofides PD. Output feedback control of switched nonlinear systems using multiple Lyapunov functions. *Systems & Control Letts*. 2005;54:1163–1182.
37. El-Farra NH, Mhaskar P, Christofides PD. Hybrid predictive control of nonlinear systems: Method and applications to chemical processes. *Intl J of Robust & Nonlinear Control*. 2004;14:199–225.
38. Mhaskar P, Gani A, Christofides PD. Fault-tolerant control of nonlinear processes: Performance-based reconfiguration and robustness. *Int J of Robust & Nonlinear Control*. 2006;16:91–111.
39. Gani A, Mhaskar P, Christofides PD. Fault-tolerant control of a gas-phase polyethylene reactor. *J of Process Control*. 2007; in press. DOI: 10.1016/j.jprocont.2006.04.002.
40. El-Farra NH, Christofides PD. Integrating robustness, optimality, and constraints in control of nonlinear processes. *Chem Eng Sci*. 2001;56:1841–1868.
41. El-Farra NH, Christofides PD. Bounded robust control of constrained multivariable nonlinear processes. *Chem Eng Sci*. 2003;58:3025–3047.
42. Mhaskar P, El-Farra NH, Christofides PD. Predictive control of switched nonlinear systems with scheduled mode transitions. *IEEE Transactions on Automatic Control*. 2005;50:1670–1680.
43. Mhaskar P, El-Farra NH, Christofides PD. Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. *Systems & Control Letts*. 2006;55:650–659.
44. Mhaskar P, Gani A, El-Farra NH, McFall C, Christofides PD, Davis JF. Integrated fault-detection and fault-tolerant control for process systems. *AIChE J*. 2006;52:2129–2148.
45. El-Farra NH, Gani A, Christofides PD. Fault-tolerant control of process systems using communication networks. *AIChE J*. 2005;51: 1665–1682.
46. Mhaskar P, El-Farra NH, Christofides PD. Robust hybrid predictive control of nonlinear systems. *Automatica*. 2005;41:209–217.
47. Patton RJ. Fault-tolerant control systems: The 1997 situation. In: Proceedings of the IFAC Symposium SAFEPROCESS 1997. Hull, U. K.; 1997:1033–1054.
48. Hassibi A, Boyd SP, How JP. Control of asynchronous dynamical systems with rate constraints on events. In: *Proceedings of 38th IEEE Conference on Decision and Control. Phoenix, AZ;* 1999:1345–1351.
49. Kravaris C, Arkun Y. Geometric nonlinear control—an overview. In: *Proceedings of 4th Intl Conference on Chemical Process Control*. Padre Island, TX; 1991:477–515.
50. Ydstie BE. Certainty equivalence adaptive control: Paradigms puzzles and switching. In: *Proceedings of 5th Intl Conference on Chemical Process Control*. Tahoe City, CA; 1997:9–23.
51. Christofides PD, El-Farra NH. *Control of nonlinear and hybrid process systems: Designs for uncertainty, constraints and time-delays*. New York: Springer; 2005.
52. El-Farra NH, Christofides PD. Coordinating feedback and switching for control of hybrid nonlinear processes. *AIChE J*. 2003;49: 2079–2098.

Manuscript received Jun. 9, 2006, and revision received Dec. 7, 2006.