INTEGRATED FAULT-DETECTION AND FAULT-TOLERANT CONTROL OF PROCESS SYSTEMS

Prashant Mhaskar, **Adiwinata Gani**,
Nael H. El-Farra, **Panagiotis D. Christofides** and
James F. Davis

Department of Chemical Engineering
University of California, Los Angeles, CA 90095

Abstract: This work considers the problem of fault-tolerant control of nonlinear processes with input constraints subject to control system/actuator failures, and presents and demonstrates an approach to fault-tolerant control predicated upon the idea of integrating fault-detection, feedback and supervisory control. Specifically, a nonlinear observer is initially designed to generate estimates of the states that are used to implement Lyapunov-based state feedback controllers and a fault-detection filter. The fault-detection filter uses the state estimates to compute the expected closed–loop behavior in the absence of faults, and detects the occurrence of faults by comparing the expected behavior of the process variables with the estimates. A switching policy is then derived to orchestrate the activation/deactivation of the constituent control configurations to achieve fault-tolerant control in the event that a failure is detected. Finally, simulation studies are presented to demonstrate the implementation and evaluate the effectiveness of the proposed fault-tolerant control scheme. *Copyright©2005 IFAC.*

Keywords: Fault-tolerant control, fault-detection, state estimation, input constraints, stability region, Lyapunov-based control.

1. INTRODUCTION

Modern-day chemical plants involve a complex arrangement of processing units, highly integrated with respect to material and energy flows through recycle streams. Increasingly faced with the requirements of safety, reliability and profitability, chemical plant operation is relying extensively on highly automated process control systems. Automation, however, tends to also increase vulnerability of the plant to faults (e.g., defects/malfunctions actuators, failures in the controllers or in the control loops) potentially causing a host of economic, environmental, and safety problems that can seriously degrade the operating efficiency of the plant if not addressed within a time appropriate to the context of the process dynamics. In the absence of an appropriate response, these faults can potentially cause a host of economic, environmental and safety problems.

These considerations provide a strong motivation for the development of systematic methods and strategies for the design of fault-tolerant control systems. In process control, given the complex dynamics of chemical processes (e.g., nonlinearities, uncertainties and constraints) and the geographically distributed, interconnected nature of plant units, the success of any fault-tolerant control method requires an integrated approach that brings together several essential elements, including: (1) the design of advanced feedback control algorithms that handle complex dynamics effectively, (2) the quick detection of process faults, and (3) the design of supervisory switching schemes that orchestrate the transition from the failed control configuration to available well-functioning fall-back configurations to ensure fault-tolerance. The realization of such an approach is increasingly aided by a confluence of recent, and ongoing, advances in several areas of process control research, including advances in nonlinear controller designs (e.g., (El-Farra and Christofides, 2001*a*; El-Farra *et al.*, 2004; Mhaskar *et al.*, 2004)), advances in the analysis and control of hybrid process systems (e.g., (Bemporad and Morari, 1999; El-Farra and Christofides, 2003)) and advances in fault-detection.

The occurrence of faults in chemical processes and subsequent switching to fall-back control configurations naturally results in the superposition of discrete events on the continuous process dynamics giving rise to an overall process behavior that is more appropriately viewed as a hybrid process, i.e., intervals of piecewise continuous behavior interspersed by discrete transitions. A hybrid systems framework therefore provides a natural setting for the analysis and design of fault-tolerant control systems. A common example is the problem of actuator/sensor failure where, upon the detection of faults in a given actuator/sensor configuration, it is often necessary to reconfigure the control system by switching to some fall-back configuration in order to preserve stability of the closed-loop system. This approach was employed in (El-Farra *et al.*, 2005), where upon occurrence of a fault, stability region-based reconfiguration is done to achieve fault-tolerant control. The reconfiguration in (El-Farra *et al.*, 2005), however, assumes full state measurements and knowledge of fault occurrence.

The success of any fault-tolerant control system relies on the ability to detect the occurrence of a fault from the available process measurements. The analytical approach to fault-detection relies on the use of fundamental models for the construction of residuals, that capture some measure of the difference between normal and 'faulty' dynamics, for fault-detection. The problem of using process models for the purpose of detecting faults has been studied extensively in the context of linear systems (Frank, 1990; Garcia and Frank, 1997; Zad and Massoumnia, 1999; Mehranbod *et al.*, 2005); and recently, some existential results in the context of nonlinear systems have been derived (Saberi *et al.*, 2000; DePersis and Isidori, 2002).

In summary, a close study of the existing literature indicates the lack of general and practical methods for the design of integrated fault-detection and fault-tolerant control structures for chemical plants accounting explicitly for actuator/controller failures, process nonlinearities and input constraints. Motivated by these considerations, in this work, we propose a methodology for the design of integrated fault-tolerant and fault-detection systems for nonlinear processes with actuator constraints. The basic idea is that of integrating fault-detection, feedback control and logic-based switching between multiple constrained control configurations, each characterized by a different manipulated input and a different region of closed-loop stability. A fault-detection filter is designed for each control configuration. The switching policy, which is based on the stability regions, is implemented by a higher-level supervisor that, upon detecting a fault in the feedback system, activates/deactivates the appropriate control configuration in a way that ensures actuator fault-tolerance. The efficacy and implementation of the proposed approach are demonstrated through a chemical process example. Detailed theoretical development and results of the proposed approach can be found in (Mhaskar *et al.*, 2005)

2. PRELIMINARIES

2.1 System description - problem formulation

We consider nonlinear processes with constraints on the manipulated input, represented by the following state-space description:

$$\begin{aligned}\dot{x}(t) &= f(x(t)) + g_{k(t)}(x(t))(u_{k(t)} + m_{k(t)})\\ y_m &= h_m(x)\\ |u_{k(t)}| &\leq u^k_{max}\\ k(t) &\in \mathcal{K} = \{1, \cdots, N\}, \;\; N < \infty\end{aligned} \tag{1}$$

where $x(t) \in \mathbb{R}^n$, $y_m \in \mathbb{R}$ denote the vector of process state and measured variables, respectively, $u_k(t) \in [-u_k^{max}, u_k^{max}] \subset \mathbb{R}$ denotes the constrained manipulated input associated with the k-th control configuration and $m_{k(t)} \in \mathbb{R}$ denotes the fault in the k-th control configuration. $k(t)$, which takes values in the finite index set $\mathcal{K}$, represents a discrete state that indexes the vector field $g_k(\cdot)$ as well as the manipulated input $u_k(\cdot)$. For each value that k assumes in $\mathcal{K}$, the process is controlled via a different manipulated input which defines a given control configuration. Switching between the available N control configurations is controlled by a higher-level supervisor, that determines $k(t)$, ensuring that only one control configuration is active at any given time, and that only a finite number of switches take place over any finite interval of time.

It is assumed that the origin is the equilibrium point of the nominal process (i.e., $f(0) = 0$), $g_k(x) \neq 0 \; \forall \; x \in \mathbb{R}^n$, and that the vector functions $f(\cdot)$ and $g_k(\cdot)$ are sufficiently smooth, for all k, on $\mathbb{R}^n$. The notation $\|\cdot\|$ is used to denote the standard Euclidean norm of a vector, the notation $|\cdot|$ is used to denote the absolute value of a scalar and x' denotes the transpose of x. 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 right, i.e., $x(T^+) = \lim\limits_{t \to T^+} x(t)$. Throughout the manuscript, we assume that for any $|u_k| \leq u^k_{max}$ the solution of the system of Eq.1 exists and is continuous for all t.

2.2 Motivating example

To motivate our fault-tolerant control system design methodology (presented in section 3), we introduce in this section a benchmark chemical reactor example that will be used throughout the paper to illustrate the design and implementation of the fault-tolerant control system. To this end, consider a well-mixed, non-isothermal continuous stirred tank reactor where three parallel irreversible elementary exothermic reactions of the form $A \overset{k_1}{\to} B$, $A \overset{k_2}{\to} U$ and $A \overset{k_3}{\to} R$ take place, where A is the reactant species, B is the desired product and U, R are undesired byproducts, and measurements of C_A are available. 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:

$$\begin{aligned}
\frac{dT}{dt} &= \frac{F}{V}(T_{A0} - T) + \sum_{i=1}^{3} R_i(C_A, T) + \frac{Q}{\rho c_p V} \\
\frac{dC_A}{dt} &= \frac{F}{V}(C_{A0} - C_A) - \sum_{i=1}^{3} k_{i0} e^{\frac{-E_i}{RT}} C_A \qquad (2) \\
\frac{dC_B}{dt} &= -\frac{F}{V} C_B + k_{10} e^{\frac{-E_1}{RT}} C_A
\end{aligned}$$

where $R_i(C_A, T) = \frac{(-\Delta H_i)}{\rho c_p} k_{i0} e^{\frac{-E_i}{RT}} C_A$, C_A and C_B denote the concentrations of the species A and B, T denotes the temperature of the reactor, Q denotes 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, and c_p and ρ denote the heat capacity and density of the reactor, respectively. The values of the process parameters and the corresponding steady-state values can be found in (Mhaskar *et al.*, 2005). It was verified that under these conditions, the process of Eq.2 has three steady-states (two locally asymptotically stable and one unstable at $(T_s, C_{As}, C_{Bs}) = (388\ K, 3.59\ kmol/m^3, 0.41\ kmol/m^3)$).

The control objective considered here is the one of stabilizing the reactor at the (open-loop) unstable steady-state. Operation at this point is typically sought to avoid high reactor temperature, while simultaneously achieving reasonable conversion. To accomplish this objective in the presence of control system failures, we consider the following manipulated input candidates (see Fig.1):

(1) Rate of heat input, $u_1 = Q$, subject to $|Q| \leq u^1_{max} = 748\ KJ/s$.
(2) Inlet stream temperature, $u_2 = T_{A0} - T_{A0s}$, subject to $|u_2| \leq u^2_{max} = 100$ K.
(3) Inlet reactant concentration, $u_3 = C_{A0} - C_{A0s}$, subject to $|u_3| \leq u^3_{max} = 4\ kmol/m^3$.

Each of the above manipulated inputs, together with measurements of reactor temperature and/or concentration, represents a unique control configuration (or control-loop) that, by itself, can stabilize the reactor. The first loop involving the heat input, Q, will be considered as the primary configuration. In the event of some failure in this configuration, however, the plant supervisor, will have to detect that a fault has occurred, using the available measurements, and then will have to activate one of the other two backup configurations in order to maintain closed-loop stability. The important questions, which we address in the next section, are how can the supervisor detect a fault, and which control loop to activate once failure is detected in the active configuration.

3. INTEGRATED FAULT DETECTION AND FAULT-TOLERANT CONTROL

Having identified the candidate control configurations that can be used, we outline in this section the main steps involved in the fault-tolerant control system design procedure. These include: 1) the synthesis of a stabilizing output feedback controller for each control configuration, 2) the explicit characterization of the constrained stability region associated with each configuration, 3) the synthesis of a fault-detection filter, and 4) the design of a switching law that orchestrates the re-configuration of the control system in a way that guarantees closed-loop stability in the event a failure is detected in the active control configuration. Below is a brief description of each step as applied to the chemical reactor example of section 2.2.

(a) *Constrained output feedback controller:* In this step, we synthesize, for each control configuration, an output feedback controller that enforces asymptotic closed-loop stability in the presence of actuator constraints. In the case of Eq.2, a simplification can be obtained by noting that C_B does not affect the evolution of either T or C_A, and therefore the controller design can be addressed on the basis of the T and C_A equations only. A controller that stabilizes the (T, C_A) system will automatically stabilize the full system. While our control objective is to achieve full state stabilization (and not output tracking), controlled outputs are introduced to facilitate transforming the system of Eq.2 into a form more suitable for explicit controller synthesis. To generate the estimates of the states from the available measurements of C_A (which are required for the implementation of the state feedback control designs), we define $y_m = C_A - C_{As}$, and for the first two control configurations, we use an observer of the form:

$$\dot{\tilde{y}} = \begin{bmatrix} -L_i a_1^i & 1 \\ -L_i^2 a_2^i & 0 \end{bmatrix} \tilde{y} + \begin{bmatrix} L_i a_1^i \\ L_i^2 a_2^i \end{bmatrix} y_m \qquad (3)$$

where $i = 1, 2$. This observer design generates $\tilde{y}_1 = \hat{C}_A$ as an estimate of C_A while $\tilde{y}_2$ is an estimate of $\dot{C}_A$, using which $\hat{T}$ is computed. For the third configuration, the estimates are generated as follows:

$$\begin{aligned} \frac{d\hat{T}}{dt} &= \frac{F}{V}(T_{A0} - \hat{T}) + \sum_{i=1}^{3} R_i(\hat{C}_A, \hat{T}) \\ &\quad + \frac{Q}{\rho c_p V} + \alpha_1(C_A - \hat{C}_A) \\ \frac{d\hat{C}_A}{dt} &= \frac{F}{V}(C_{A0} - \hat{C}_A) - \sum_{i=1}^{3} k_{i0} e^{\dfrac{-E_i}{R\hat{T}}} \hat{C}_A \\ &\quad + \alpha_2(C_A - \hat{C}_A) \end{aligned} \qquad (4)$$

where α_1, α_2 are real numbers, and $\hat{T}$, $\hat{C}_A$ are estimates of T and C_A, respectively. These estimates are used in conjunction with the state feedback control designs presented below.

1. For the first configuration with $u_1 = Q$, we consider the controlled output $y_1 = C_A - C_{As}$. This choice yields a relative degree of $r_1 = 2$ for the controlled output with respect to the manipulated input. The coordinate transformation (in error variables form) takes the form: $e_1 = C_A - C_{As}$, $e_2 = \frac{F}{V}(C_{A0} - C_A) - \sum_{i=1}^{3} k_{i0} e^{\frac{-E_i}{RT}} C_A$.

2. For the second configuration with $u_2 = T_{A0} - T_{A0s}$, we choose the output $y_2 = C_A - C_{As}$ which yields the same relative degree as in the first configuration, $r_2 = 2$, and the same coordinate transformation.

3. For the third configuration with $u_3 = C_{A0} - C_{A0s}$, a coordinate transformation of the form used for configurations 1 and 2 above does not yield a sufficiently large estimate of the stability region, we therefore choose a candidate Lyapunov function of the form $V_3(x) = x'Px$, where $P > 0$ and $x = [T - T_s \quad C_A - C_{As}]'$ with $P = \begin{Bmatrix} 0.011 & 0.019 \\ 0.019 & 0.101 \end{Bmatrix}$.

Note that since our objective is full state stabilization, the choice of the controlled output in each case is really arbitrary. However, to facilitate our controller design and subsequent stability analysis, we have chosen in each case a controlled output that produces a system of relative degree 2. For the first and second configurations, the corresponding state transformation yields a system, describing the input/output dynamics, of the following form:

$$\begin{aligned} \dot{e} &= Ae + l_k(e) + b\alpha_k u_k \\ &:= \bar{f}_k(e) + \bar{g}_k(e) u_k \end{aligned} \qquad (5)$$

where $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $b = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $l_k(\cdot) = L_{f_k}^2 h_k(x)$, $\alpha_k(\cdot) = L_{g_k} L_{f_k} h_k(x)$, $h_k(x) = y_k$ is the output associated with the k-th configuration, $x = [x_1 \; x_2]^T$ with $x_1 = T - T_s$, $x_2 = C_A - C_{As}$, and the functions $f_k(\cdot)$ and $g_k(\cdot)$ can be obtained by re-writing the (T, C_A) model equations in Eq.2 in the form of Eq.1. The explicit forms of these functions are omitted for brevity. Using a quadratic Lyapunov function of the form $V_k = e^T P_k e$, where P_k is a positive-definite symmetric matrix that satisfies the Riccati inequality $A^T P_k + P_k A - P_k b b^T P_k < 0$, we synthesize, for each control-loop, a bounded nonlinear feedback control law (see (Lin and Sontag, 1991; El-Farra and Christofides, 2001*b*; El-Farra and Christofides, 2001*a*; Christofides and El-Farra, 2005)) of the form:

$$u = -r(x, u_{max}^k) L_{\bar{g}_k} V_k \qquad (6)$$

where $r(x, u_{max}^k) =$

$$\frac{L_{\bar{f}_k}^* V_k + \sqrt{(L_{\bar{f}_k}^* V_k)^2 + (u_{max}^k |L_{\bar{g}_k} V_k|)^4}}{(|L_{\bar{g}_k} V_k|)^2 \left[1 + \sqrt{1 + (u_{max}^k |L_{\bar{g}_k} V_k|)^2}\right]} \qquad (7)$$

and $L_{\bar{f}_k}^* V_k = L_{\bar{f}_k} V_k + \rho |e|^2$, $\rho > 0$. The characterization of the stability region for this controller is discussed in the next step.

(b) *Characterization of stability regions:* Given that actuator constraints place fundamental limitations on the initial conditions that can be used for stabilization, it is important for the control system designer to explicitly characterize these limitations by identifying, for each control configuration, the set of admissible initial conditions starting from where the constrained closed-loop system is asymptotically stable. As discussed in step (c) below, this characterization is necessary for the design of an appropriate switching policy that ensures the fault-tolerance of the control system. The control law designed in step (a) provides such a characterization. Consider the set:

$$\Theta(u_{max}^k) = \{x \in \mathrm{I\!R}^n : L_{\bar{f}_k}^* V_k \le u_{max}^k |L_{\bar{g}_k} V_k|\} \qquad (8)$$

Then, using Lyapunov arguments, it can be shown that an invariant subset of $\Theta(u_{max}^k)$, $\Omega(u_{max}^k)$ provides an estimate of the stability region for the k-th control configuration (see (El-Farra and Christofides, 2001*a*) for more details on this issue). The fact that the state feedback controllers are implemented using the state estimates requires appropriate design of the observer so that a chosen subset of the state feedback stability region Ω can be used as the output feedback stability region $\hat{\Omega}$.

(c) *Fault-detection filter:* The approach employed in the filter design is to compare the expected behavior in the absence of faults, to the true behavior and use the difference between the two, as an indicator of a fault. The prediction of the expected behavior in the absence of faults, however, requires knowledge of the true values of the process states. The filter design, therefore, uses the estimates of the states generated by the state estimator to predict the behavior in the absence of faults, and compares it with the observed behavior of the system to generate a residual, $r(t)$. The presence of estimation error means, however, that $r(t) \neq 0$ even in the absence of faults. It is possible, however, to establish a bound δ_m on the residual which captures the expected difference in behavior in the absence of faults and is used as a threshold in declaring a fault. Consequently, if no fault is present, $r(t) \leq \delta_m$, while the supervisor detects faults for which $r(t) > \delta_m$. The residual is generated as:

$$r_i = \|(\hat{T}, \hat{C_A}) - (\tilde{T}, \tilde{C_A})\| \tag{9}$$

where i is the active configuration, r_i is the residual for the i-th control configuration and:

$$\begin{aligned} \frac{d\tilde{T}}{dt} &= \frac{F}{V}(T_{A0} - \tilde{T}) + \sum_{i=1}^{3} R_i(\tilde{C}_A, \tilde{T}) \\ &\quad + \frac{Q}{\rho c_p V} \\ \frac{d\tilde{C}_A}{dt} &= \frac{F}{V}(C_{A0} - \tilde{C}_A) - \sum_{i=1}^{3} k_{i0} e^{\frac{-E_i}{R\tilde{T}}} \tilde{C}_A \end{aligned} \tag{10}$$

with $\tilde{C}_A(T_d) = \hat{C}_A(T_d)$ and $\tilde{T}(T_d) = \hat{T}(T_d)$ where $T_d > 0$ is of the order of $1/L$, where L is the observer gain. Note that the fault-detection filter is initialized using the value of the state estimates after some time has elapsed to allow for the estimates to converge to the true values. Note also that both the bound on the residual and the time after which the fault-detection filter is initialized can be made as small as desired by appropriate choice of the observer gain (for more details on the filter design, see (Mhaskar *et al.*, 2005)).

(d) *Supervisory switching-logic:* The key idea in designing the switching logic is that, because of the limitations imposed by constraints on the stability region of each configuration, and the unavailability of the true state values, the supervisor can only activate the control configuration for which the closed-loop state is within the stability region at the time of control system failure, and the supervisor needs to make this inference by using the available state estimates. To this end, the supervisor first computes the sets, $\tilde{\Omega}_j$, $j = 1, \ldots, N$ such that the presence of the state estimates in $\tilde{\Omega}_j$ (after they have converged to the true state values) ensures the presence of the states in the output feedback stability region $\hat{\Omega}_j$. Without loss of generality, let the initial actuator configuration be $k(0) = 1$ and T be the time when the residual value for this configuration becomes greater than δ_m, then the switching rule given by

$$k(t) = j \; \forall \, t \geq T \; if \;\; \hat{x}(T) \in \tilde{\Omega}_j(u^j_{max}) \tag{11}$$

for some $j \in \{2, 3, \cdots, N\}$ guarantees asymptotic closed-loop stability.

4. SIMULATION RESULTS

In this section, we illustrate the implementation of the proposed fault-tolerant control methodology to the chemical reactor example introduced in section 2.2. We have already described in section 3 how the output feedback controllers can be designed and the stability regions characterized for each of the three control configurations and how the fault-detection filter is designed. Fig.1 depicts the stability region, for each configuration. For the first two control configurations, a state estimator of the form of Eq.3 is designed. For fault-detection thresholds of $\delta_m = 0.0172$ and 0.00151, the parameters in the observer of Eq.3 are chosen as $L_1 = L_2 = 100$, $a_1^{(1)} = a_1^{(2)} = 10$ and $a_2^{(1)} = a_2^{(2)} = 20$ and in the observer of Eq.4 are chosen as $\alpha_1 = -10^4$ and $\alpha_2 = 10$. The reactor is initialized at $T(0) = 330\ K$, $C_A(0) = 3.6\ kmol/m^3$, $C_B(0) = 0.0\ kmol/m^3$, using the Q-control configuration, while the state estimates are initialized at $\hat{T}(0) = 390\ K$, $\hat{C}_A(0) = 3.6\ kmol/m^3$.

The states in the fault-detection filter are initialized and set equal to the value of the state estimates at $t = 0.01$ minutes $\equiv T_1^b$; note that by this time the estimates have converged to the true values. For the purpose of comparison, if the fault detection filter was initialized at $t = 0$, it results in a false alarm (the value or $r_1(t)$ crosses the threshold before $t = 0.01$ minutes $\equiv T_1^b$ even in the absence of faults). By initializing the fault-detection filter appropriately, a false alarm is prevented (the value of $r_1(t)$ does not hit the threshold in the absence of a fault after a time $t = 0.01$ minutes, see Fig.2a). As shown by the solid lines in Fig.1, the controller proceeds to drive the closed-loop trajectory towards the desired steady-state, up until the Q-configuration fails after 3.0 minutes $\equiv T_1^f$ of reactor startup. Note that at this time, the value of $r_1(t)$ becomes non-zero and hits the threshold at $t = 3.3$ minutes $\equiv T_1^s$. From Fig.1, it is clear that the failure of the primary control configuration occurs when the closed-loop trajectory is within the stability region of the second control configuration, and outside the stability region of the third control configuration. Therefore, on the basis of the switching logic of Eq.11, the supervisor activates the second configuration (with T_{A0} as the manipulated input, see solid line in Fig.1) which continues to drive the state trajectory closer to the desired steady-state. When a second failure occurs (this time in the T_{A0}-configuration) at $t = 13.0$ minutes

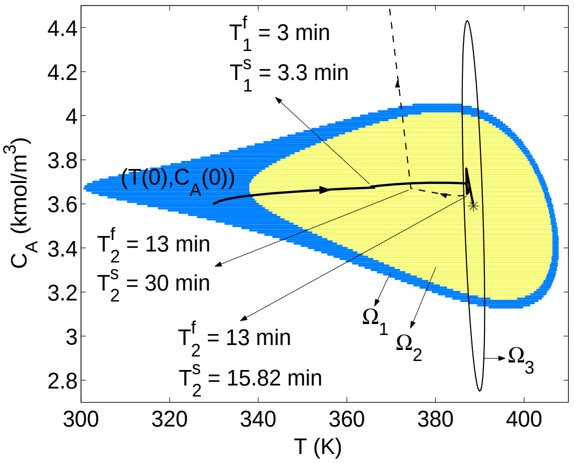
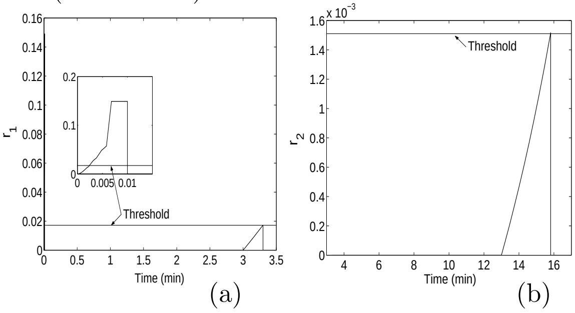


Fig. 1. Evolution of the closed-loop state trajectory under the switching rule of Eq.11 subject to failures in control systems 1 and 2, using an appropriate fault-detection filter (solid line) and in the absence of a fault-detection filter (dashed line).



(a) (b)

Fig. 2. Evolution of the residual for (a) the first control configuration and (b) the second control configuration.

$\equiv T_2^f$ before the process has reached the steady state, the filter detects this failure via the value of $r_2(t)$ hitting the threshold (see Fig.2b). From the solid line in Fig.1, it is clear that the failure of the second control configuration occurs when the closed-loop trajectory is within the stability region of the third configuration. However, if the fault-detection filter is not in place and the backup configuration is implemented late in the closed–loop (at $t = 30$ minutes $\equiv T_2^s$), by this time the state of the closed–loop system has moved out of the stability region of the third control configuration, and closed–loop stability is not achieved (see dashed line in Fig.1). In contrast, when the fault-detection filter is in place, it detects a fault at $t = 15.82$ minutes $\equiv T_2^s$ and when the supervisor switches to configuration 3, closed–loop stability is achieved (see solid line in Fig.1).

REFERENCES

Bemporad, A. and M. Morari (1999). Control of systems integrating logic, dynamics and constraints. *Automatica* **35**, 407–427.

Christofides, P. D. and N. H. El-Farra (2005). *Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-Delays,* 452 pages, to appear. Springer. New York.

DePersis, C. and A. Isidori (2002). On the design of fault detection filters with game-theoretic-optimal sensitivity. *Int. J. Rob. & Non. Contr.* **12**, 729–747.

El-Farra, N. H., A. Gani and P. D. Christofides (2005). Fault-tolerant control of process systems using communication networks, to appear. *AIChE J.*

El-Farra, N. H. and P. D. Christofides (2001*a*). Integrating robustness, optimality, and constraints in control of nonlinear processes. *Chem. Eng. Sci.* **56**, 1841–1868.

El-Farra, N. H. and P. D. Christofides (2001*b*). Robust near-optimal output feedback control of nonlinear systems. *Int. J. Contr.* **74**, 133–157.

El-Farra, N. H. and P. D. Christofides (2003). Coordinated feedback and switching for control of hybrid nonlinear processes. *AIChE J.* **49**, 2079–2098.

El-Farra, N. H., P. Mhaskar and P. D. Christofides (2004). Uniting bounded control and MPC for stabilization of constrained linear systems. *Automatica* **40**, 101–110.

Frank, P. M. (1990). Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy – a survey and some new results. *Automatica* **26**, 459–474.

Garcia, E. A. and P. M. Frank (1997). Deterministic nonlinear observer-based approaches to fault diagnosis: A survey. *Contr. Eng. Prac.* **5**, 663–670.

Lin, Y. and E. D. Sontag (1991). A universal formula for stabilization with bounded controls. *Sys. & Contr. Lett.* **16**, 393–397.

Mehranbod, N., M. Soroush and C. Panjapornpon (2005). A method of sensor fault detection and identification. *J. Proc. Contr.* **15**, 321–339.

Mhaskar, P., A. Gani, N. H. El-Farra, P. D. Christofides and J. F. Davis (2005). Integrated fault-detection and fault-tolerant control for process systems. *AIChE J.,* submitted.

Mhaskar, P., N. H. El-Farra and P. D. Christofides (2004). Hybrid predictive control of process systems. *AIChE J.* **50**, 1242–1259.

Saberi, A., A. A. Stoorvogel, P. Sannuti and H. Niemann (2000). Fundamental problems in fault detection and identification. *Inter. J. Rob. & Non. Contr.* **10**, 1209–1236.

Zad, S. H. and M. Massoumnia (1999). Generic solvability of the failure detection and identification problem. *Automatica* **35**, 887–893.