INTERNATIONAL JOURNAL OF ROBUST AND NONLINEAR CONTROL
Int. J. Robust Nonlinear Control 2006; **16**:91–111
Published online 20 December 2005 in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/rnc.1045

Fault-tolerant control of nonlinear processes: Performance-based reconfiguration and robustness

Prashant Mhaskar, Adiwinata Gani and Panagiotis D. Christofides*,†

Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, U.S.A.

SUMMARY

This work considers the problem of control system/actuator failures in nonlinear processes subject to input constraints and presents two approaches for fault-tolerant control that focus on incorporating performance and robustness considerations, respectively. In both approaches, first a family of candidate control configurations, characterized by different manipulated inputs, is identified for the process under consideration. Performance considerations are first incorporated via the design of a Lyapunov-based predictive controller that enforces closed-loop stability from an explicitly characterized set of initial conditions (computed using an auxiliary Lyapunov-based nonlinear controller). A hierarchical switching policy is derived, that uses stability considerations (evaluated via the presence of the state in the stability region of a control configuration) to ascertain the suitability of a candidate backup configuration and then performance considerations are again considered in choosing between the suitable backup configurations. Next, we consider the problem of implementing fault-tolerant control to nonlinear processes subject to input constraints and uncertainty. To this end, we first design a robust hybrid predictive controller for each candidate control configuration that guarantees stability from an explicitly characterized set of initial conditions, subject to uncertainty and constraints. A switching policy is then derived to orchestrate the activation/deactivation of the constituent control configurations. Finally, simulation studies are presented to demonstrate the implementation and evaluate the effectiveness of the proposed fault-tolerant control method. Copyright © 2005 John Wiley & Sons, Ltd.

KEY WORDS: fault-tolerant control; nonlinear systems; input constraints; model predictive control; closed-loop stability region; process control

1. INTRODUCTION

The operation of modern-day chemical plants involves an interconnection of complex processing units via material and energy flows through recycle streams. Aided by the advances in sensing, communicating and computing technologies, chemical plant operation is relying

*Correspondence to: Panagiotis D. Christofides, Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, U.S.A.
† E-mail: pdc@seas.ucla.edu

Contract/grant sponsor: National Science Foundation; contract/grant number: CTS-0529295

extensively on automated process control systems to satisfy simultaneously the (sometimes conflicting) requirements of safety, reliability and profitability. Increased automation, however, also makes the plant susceptible to faults (e.g. defects/malfunctions in process equipment, sensors and actuators, failures in the controllers or in the control loops) that can result in substantial financial losses and/or safety hazards if not addressed within a time appropriate to the context of the process dynamics.

The above considerations provide a strong motivation for the development of methods and strategies for the design of advanced fault-tolerant controllers that account for process complexities such as nonlinearity, uncertainty and constraints and provide a mechanism for an efficient and timely response to enhance fault recovery. A prerequisite for implementing fault-tolerant control is the availability of more control configurations than are required. This can be exploited by using all control loops at the same time so that failure of one control loop does not lead to the failure of the entire control structure (the reliable control approach, e.g. see Reference [1]). Another approach dictates the use of only as many control loops as is required at a time (to save on unnecessary control action) and to achieve fault-tolerance through control-loop reconfiguration in the event of failure of the primary control configuration. Using these approaches fault-tolerant control has been actively pursued in the context of aerospace engineering applications (see, e.g. References [2, 3]). Recently it has also gained attention in the context of chemical process control; however, the available results are based on the assumption of a linear process description (e.g. References [4, 5]) and do not account for process nonlinearity, constraints and uncertainty.

Even in the absence of faults, chemical process operation is often characterized by the presence of highly nonlinear behaviour which has motivated extensive research on nonlinear process control. Excellent reviews of results in the area of nonlinear process control can be found, for example, in References [6, 7]; for a more recent review, see Reference [8]. The problems caused by input constraints have motivated numerous studies on the dynamics and control of systems subject to input constraints [9–17]. Recently, we developed techniques for uniting predictive control with Lyapunov-based control that provide an explicit characterization of the stability region for the closed-loop system via switching between Lyapunov-based and predictive controllers [18–21] and via the design of Lyapunov-based predictive controllers [22, 23].

Switching to fall-back control configurations in the event of faults results in an overall process that exhibits intervals of piecewise continuous behaviour interspersed by discrete transitions. A hybrid systems framework therefore provides a natural setting for the analysis and design of fault-tolerant control structures. However, at this stage, despite the large and growing body of research work on a diverse array of hybrid system problems (e.g. References [24–30]), the use of a hybrid system framework for the study of fault-tolerant control problems has received limited attention. In Reference [31], a hybrid systems approach to fault-tolerant control was employed where upon occurrence of a fault, stability region-based reconfiguration is done to achieve fault-tolerant control. In Reference [32], the problem of implementing integrated fault-detection and fault-tolerant control was addressed for the state and output feedback cases. The reconfiguration in References [31, 32], however, does not incorporate performance or robustness considerations, which can lead to performance-loss or even instability for processes subject to uncertainty.

Motivated by these considerations, in this work we consider the problem of control system/actuator failures in nonlinear processes subject to input constraints and present two approaches for fault-tolerant control that focus on incorporating performance and robustness considerations, respectively. In both approaches, first a family of candidate control configurations, characterized by different manipulated inputs, is identified for the process under consideration, and then performance and robustness considerations are incorporated in the implementation of fault-tolerant control. The remainder of the paper is organized as follows: in Section 2, we introduce the class of systems considered, present a motivating example and review two control approaches for handling process nonlinearity, and input constraints. In Section 3.2, we present performance-based reconfiguration where performance considerations are incorporated in the controller design and in the switching logic. Specifically, we first design a Lyapunov-based predictive controller that enforces closed-loop stability from an explicitly characterized set of initial conditions. The switching logic uses stability considerations (evaluated via the presence of the state in the stability region of a control configuration) to ascertain the suitability of a candidate backup configuration and then performance considerations are again considered in choosing between the suitable backup configurations. In Section 3.3 we demonstrate the implementation of the method on the motivating example of Section 2.1. In Section 4 we consider the problem of implementing fault-tolerant control to nonlinear processes subject to input constraints and uncertainty. To this end, we first design a robust hybrid predictive controller in Section 4.1 for each candidate control configuration that guarantees stability from an explicitly characterized set of initial conditions, subject to uncertainty and constraints. A switching policy is then derived in Section 4.2 to orchestrate the activation/deactivation of the constituent control configurations. In Section 4.3 we demonstrate the implementation of the robust fault-tolerant controller and in Section 5 we summarize our results.

2. PRELIMINARIES

We consider nonlinear systems with uncertain variables and input constraints, described by

$$\begin{aligned} \dot{x} &= f(x) + G_k(x)u_k + W_k(x)\theta_k(t), \quad u_k \in \mathbf{U}_k, \quad \theta_k \in \Theta_k \\ k(t) &\in \mathcal{K} = \{1, \ldots, N\}, \quad N < \infty \end{aligned} \tag{1}$$

where $x \in \mathbb{R}^n$ denotes the vector of state variables, $u \in \mathbb{R}^m$ denotes the vector of constrained manipulated inputs, taking values in a non-empty convex subset $\mathbf{U}_k$ of $\mathbb{R}^m$, where $\mathbf{U}_k = \{u \in \mathbb{R}^m : \|u\| \leqslant u_k^{\max}\}$, $\|\cdot\|$ is the Euclidean norm of a vector, $u_k^{\max} > 0$ is the magnitude of input constraints, and $\theta_k(t) = [\theta_k^1(t) \cdots \theta_k^q(t)]^{\mathrm{T}} \in \Theta_k \subset \mathbb{R}^q$ denotes the vector of uncertain (possibly time-varying) but bounded variables taking values in a non-empty compact convex subset of $\mathbb{R}^q$ and $f(0) = 0$. The vector function $f(x)$, the matrices $G_k(x) = [g_k^1(x) \cdots g_k^m(x)]$ and $W(x) = [w_k^1(x) \cdots w_k^q(x)]$, where $g_k^i(x) \in \mathbb{R}^n$, $i = 1 \ldots m$, and $w_k^i(x) \in \mathbb{R}^n$, $i = 1 \ldots q$, 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 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, thus determining the temporal evolution of the discrete state, $k(t)$. The supervisor ensures that only one control configuration is active at any given time, and allows only a finite number of switches over any finite interval of time. The notation $L_f h$ denotes the standard Lie derivative of a scalar function

$h(\cdot)$ with respect to the vector function $f(\cdot)$, the notation $x(T^-)$ denotes the limit of the trajectory $x(t)$ as T is approached from the left, i.e. $x(T^-) = \lim_{t\to T^-} x(t)$ and the notation $\partial\Omega$ is used to denote the boundary of a closed set, Ω. Throughout the manuscript, we assume that for any $u_k \in \mathbf{U}_k$ the solution of the system of Equation (1) exists and is continuous for all t, and we focus on the state feedback control problem where measurements of the entire state, $x(t)$, are assumed to be available for all t.

2.1. Motivating example

To illustrate how performance and robustness considerations are incorporated in the fault-tolerant control design, we introduce in this subsection a benchmark chemical reactor example (also used in References [31, 32]). Specifically, consider a well-mixed, non-isothermal continuous stirred tank reactor where three parallel irreversible elementary exothermic reactions of the form $A \to^{k_1} B$, $A \to^{k_2} U$ and $A \to^{k_3} R$ 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}. A mathematical model of the process takes the following form:

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

where C_A and C_B denote the concentrations of the species A and B, 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, and c_p and ρ denote the heat capacity and density of the fluid in the reactor, respectively. The values of the process parameters and the corresponding steady state values are given in Table I. It was verified that under these conditions, the open-loop process of Equation (2) has three steady states (two locally asymptotically stable and one unstable at $(T_s, C_{As}, C_{Bs}) = (388.57\ \text{K}, 3.59\ \text{kmol/m}^3, 0.41\ \text{kmol/m}^3)$). Operation at the (open-loop) unstable steady state is typically sought to avoid high temperatures, while simultaneously achieving reasonable conversion. Therefore, the control objective considered here is the one of stabilizing the reactor at the (open-loop) unstable steady state. The manipulated input variables available for use within a control configuration include (see Figure 1) rate of heat input, $u_1 = Q$, inlet stream temperature, $u_2 = T_{A0} - T_{A0s} := \Delta T_{A0}$ and inlet reactant concentration, $u_3 = C_{A0} - C_{A0s} := \Delta C_{A0}$, subject to the constraints $|Q| \leqslant u_1^{\max} = 748$ K J/s, $|u_2| \leqslant u_2^{\max} = 100$ K, with $T_{A0s} = 300$ K and $|u_3| \leqslant u_3^{\max} = 4\ \text{kmol/m}^3$, with $C_{A0s} = 4\ \text{kmol/m}^3$, respectively.

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 activate one of the other two backup configurations in order to maintain closed-loop stability. Note, however, that the presence of constraints on the manipulated inputs limits the set of initial conditions starting from where the process states can be driven to a given (open-loop unstable)

Table I. Parameter values and units.

$F = 4.998\ \mathrm{m}^3/\mathrm{h}$
$V = 1.0\ \mathrm{m}^3$
$R = 8.314\ \mathrm{kJ/kmol\,K}$
$T_{A0} = 300.0\ \mathrm{K}$
$C_{A0} = 4.0\ \mathrm{kmol/m}^3$
$C_{B0} = 0.0\ \mathrm{kmol/m}^3$
$\Delta H_1 = -5.0 \times 10^4\ \mathrm{k\,J/kmol}$
$\Delta H_2 = -5.2 \times 10^4\ \mathrm{k\,J/kmol}$
$\Delta H_3 = -5.4 \times 10^4\ \mathrm{k\,J/kmol}$
$k_{10} = 3.0 \times 10^6\ \mathrm{h}^{-1}$
$k_{20} = 3.0 \times 10^5\ \mathrm{h}^{-1}$
$k_{30} = 3.0 \times 10^5\ \mathrm{h}^{-1}$
$E_1 = 5.0 \times 10^4\ \mathrm{k\,J/kmol}$
$E_2 = 7.53 \times 10^4\ \mathrm{k\,J/kmol}$
$E_3 = 7.53 \times 10^4\ \mathrm{k\,J/kmol}$
$\rho = 1000.0\ \mathrm{kg/m}^3$
$c_p = 0.231\ \mathrm{kJ/kg\,K}$
$T^s = 388.57\ \mathrm{K}$
$C_A^s = 3.59\ \mathrm{kmol/m}^3$
$C_B^s = 0.41\ \mathrm{kmol/m}^3$

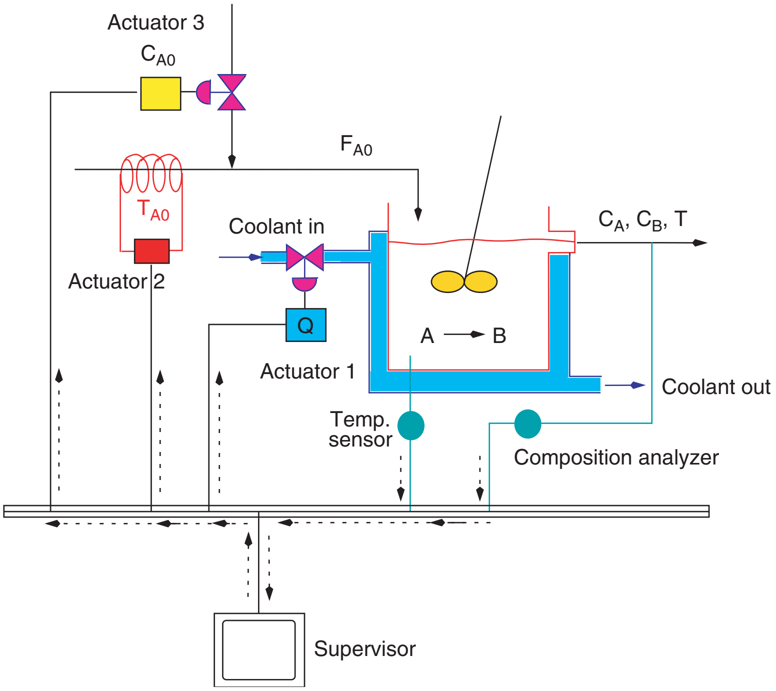

Figure 1. A schematic of the CSTR showing the three candidate control configurations.

equilibrium point. Given that the primary control configuration fails, it is important to pick the appropriate backup control configuration that preserves closed-loop stability (safety criterion), and upon availability of more than one backup control configurations that satisfy the safety criterion, to formulate and evaluate a performance index to choose between them (performance consideration). To this end, for each individual control configuration subject to constraints, it is important to implement control laws that provide an explicit estimate of the set of initial conditions starting from where closed-loop stability can be achieved. Such estimates of the stability region can subsequently be used to evaluate the suitability of a given backup control configuration.

Lyapunov-based nonlinear controllers are an example of such controllers that provide an explicit estimate of the stability regions. These controllers, however, are typically not designed to be optimal with respect to arbitrarily specified performance criterion. Model predictive controllers, while typically not allowing for an explicit characterization of their stability region, allow for incorporation of performance considerations, via the objective function or as constraints on the state variables. In the remainder of the paper, we will use a combination of analytical and predictive approaches, at the level of design and analysis (Section 3.1) or via directly switching between the two control approaches (Section 4.1) for incorporating performance (Section 3.2) and robustness (Section 4.2) considerations in fault-tolerant control of processes. We next review an example of a Lyapunov-based nonlinear controller followed by a representative description of the model predictive control approach.

2.2. *Bounded Lyapunov-based control*

Referring to the system of Equation (1), for a fixed value of $k \in \mathcal{K}$, we assume that the uncertain variable term, $W_k(x)\theta_k$, is non-vanishing (in the sense that the origin is no longer the equilibrium point of the uncertain system) and that a robust control Lyapunov function (RCLF [33]), V_k exists. Consider also, the bounded state feedback control law (see References [15, 29] for details on controller design):

$$u_k^b = -\left(\frac{\alpha_k(x) + \sqrt{(\alpha_{1,k}(x))^2 + (u_k^{\max}\beta_k(x))^4}}{(\beta_k(x))^2[1 + \sqrt{1 + (u_k^{\max}\beta_k(x))^2}]}\right)(L_{G_k}V_k)^{\mathrm{T}} := b_k(x) \tag{3}$$

when $L_{G_k}V_k \neq 0$ and $u_k = 0$ when $L_{G_k}V_k = 0$, where $\alpha_k(x) = L_f V_k + (\rho_k\|x\| + \chi_k\theta_k^b\|L_{W_k}V_k\|)(\|x\|/(\|x\| + \phi_k))$, $\alpha_{1,k}(x) = L_f V_k + \rho_k\|x\| + \chi_k\theta_k^b\|L_{W_k}V_k\|$, $\beta_k(x) = \|(L_{G_k}V_k)^{\mathrm{T}}\|$, $L_{G_k}V_k = [L_{g_k^1}V_k \cdots L_{g_k^m}V_k]$ and $L_{W_k}V_k = [L_{w_k^1}V_k \cdots L_{w_k^q}V_k]$ are row vectors, θ_k^b is a positive real number such that $\|\theta_k(t)\| \leqslant \theta_k^b$, for all $t \geqslant 0$, and ρ_k, χ_k and ϕ_k are adjustable parameters that satisfy $\rho_k > 0$, $\chi_k > 1$ and $\phi_k > 0$. Let Π_k be the set defined by $\Pi_k(\theta_k^b, u_k^{\max}) = \{x \in \mathbb{R}^n : \alpha_{1,k} \times (x) \leqslant u_k^{\max}\beta_k(x)\}$ and assume that $\Omega_k := \{x \in \mathbb{R}^n : V_k(x) \leqslant c_k^{\max}\} \subseteq \Pi_k(\theta_k^b, u_k^{\max})$ for some $c_k^{\max} > 0$. Then, given any positive real number, d_k^r, such that:

$$\mathbb{D}_k^r := \{x \in \mathbb{R}^n : \|x\| \leqslant d_k^r\} \subset \Omega_k \tag{4}$$

and for any initial condition $x_0 \in \Omega_k$, it can be shown that there exists a positive real number ε_k^{r*} such that if $\phi_k/(\chi_k - 1) < \varepsilon_k^{r*}$, the states of the closed-loop system of Equations (1) and (3) satisfy $x(t) \in \Omega_k \ \forall t \geqslant 0$ and $\limsup_{t\to\infty} \|x(t)\| \leqslant d_k^r$.

Remark 1

Referring to the above controller design, it is important to note that a general procedure for the construction of RCLFs for nonlinear systems of the form of Equation (1) is currently not available. Yet, for several classes of nonlinear systems that arise commonly in the modeling of engineering applications, it is possible to exploit system structure to construct RCLFs (see, for example, References [33, 34]). Note also that the computation of the stability region above only involves algebraic computations, and furthermore, for implementation purposes, the entire stability region information is contained in the value of the level set $c_k^{\max}$ which defines the boundary of the stability region. The presence of a given initial condition in the stability region can be ascertained by simply checking the value of the Lyapunov function for the given initial condition against $c_k^{\max}$ ($V(x(0)) \leqslant c_k^{\max}$ implies $x(0) \in \Omega_k$). Note also that possibly larger estimates of the stability region can be computed using constructive procedures such as Zubov's method [35] or by using a combination of several Lyapunov functions.

2.3. Model predictive control

The model predictive control approach provides a framework with the ability to handle, among other issues, multi-variable interactions, constraints on controls, and optimization requirements, all in a consistent, systematic manner. For the purpose of illustrating our results, we describe here a symbolic MPC formulation that incorporates most existing MPC formulations as special cases. In MPC, the control action at time t is conventionally obtained by solving, on-line, a finite horizon optimal control problem. The generic form of the optimization problem can be described as

$$\begin{aligned} u_k(\cdot) &= \text{argmin}\{\max\{J_s(x,t,u_k(\cdot))|\theta_k(\cdot) \in \Theta_k\}|u_k(\cdot) \in S_k\} := M_k \\ \text{s.t.} \quad & \dot{x}(t) = f(x(t)) + G_k(x)u_k + W_k(x)\theta_k(t) \\ & x(0) = x_0, \quad x(t+T_k) \in \Omega_{\text{MPC}}(x,t,\theta_k) \\ J_s(x,t,u_k(\cdot)) &= \int_t^{t+T_k} (x'(s)Q_k x(s) + u'(s)R_k u(s))\,\mathrm{d}s + F_k(x(t+T_k)) \end{aligned} \tag{5}$$

and $S_k = S_k(t,T)$ is the family of piecewise continuous functions, with period Δ_k, mapping $[t, t+T_k]$ into the set of admissible controls, T_k is the horizon length and θ_k is the bounded uncertainty assumed to belong to a set Θ_k. A control $u_k(\cdot)$ in S_k is characterized by the sequence $\{u_k[j]\}$ where $u_k[j] := u_k(j\Delta)$ and satisfies $u_k(t) = u_k[j]$ for all $t \in [j\Delta_k, (j+1)\Delta_k)$. J_s is the performance index, R_k and Q_k are strictly positive definite, symmetric matrices and the function $F_k(\cdot)$ represents a penalty on the states at the end of the horizon. The maximization over θ_k may not be carried out if the MPC version used is not a min–max type of formulation. The set $\Omega_{\text{MPC}}(x,t,\theta_k)$ could be a fixed, terminal set, or may represent inequality constraints (as in the case of MPC formulations that require some norm of the state, or a Lyapunov function for the system, to decrease at the end of the horizon). This stability constraint may or may not account for uncertainty. The stability guarantees in MPC formulations (with or without explicit stability conditions, and with or without robustness considerations, and whether or not it is a min–max type of formulation) are dependent on the assumption of initial feasibility. Obtaining an explicit characterization of the closed-loop stability region of the predictive controller under uncertainty and constraints remains a difficult task.

3. FAULT-TOLERANT CONTROL: PERFORMANCE-BASED RECONFIGURATION

To clearly illustrate the main idea behind incorporating performance considerations in fault-tolerant control of processes, in this section we consider processes without uncertainty. The performance considerations are incorporated both at the lower-level; by using a predictive control design described in Section 3.1 that incorporates performance objectives without sacrificing the explicit characterization of the stability region (essential to implementing fault-tolerant control in the proposed method) and also at the upper-level; by incorporating performance considerations in the switching rule (described in Section 3.2).

3.1. Lyapunov-based predictive control

We review here a Lyapunov-based design of MPC that guarantees feasibility of the optimization problem and hence constrained stabilization of the closed-loop system from an explicitly characterized set of initial conditions (for more details, see Reference [22]). Preparatory to the characterization of the stability properties of the Lyapunov-based predictive controller, we first present a proposition stating the stability properties of the bounded controller of Equation (3). Specifically, the bounded controller of Equation (3) possesses a robustness property with respect to measurement errors, that preserves closed-loop stability when the control action is implemented in a discrete (sample and hold) fashion with a sufficiently small hold time (Δ). The control law ensures that, for all initial conditions in Ω_k, the closed-loop state remains in Ω_k and eventually converges to some neighbourhood of the origin whose size depends on Δ. This robustness property, stated below in Proposition 1, is exploited in the Lyapunov-based predictive controller design (for a proof, see Reference [22]). For further results on the analysis and control of sampled-data nonlinear systems, the reader may refer to References [36–39].

Proposition 1

Consider the constrained system of Equation (1) for a fixed value of k with $\theta_k(t) = 0\ \forall t \geqslant 0$, under the bounded control law of Equation (3) designed using the Lyapunov function V_k and $\rho_k > 0$, and the stability region estimate Ω_k under continuous implementation. Let $u_k(t) = u_k(j\Delta_k)$ for all $j\Delta_k \leqslant t < (j+1)\Delta_k$ and $u_k(j\Delta_k) = b_k(x(j\Delta_k))$, $j = 0, \ldots, \infty$. Then, given any positive real number d_k, there exist positive real numbers Δ_k^*, δ_k' and ε_k^* such that if $\Delta_k \in (0, \Delta_k^*]$ and $x(0) := x_0 \in \Omega_k$, then $x(t) \in \Omega_k\ \forall t \geqslant 0$ and $\limsup_{t\to\infty} \|x(t)\| \leqslant d_k$. Also, if $V_k(x_0) \leqslant \delta_k'$ then $V_k(x(\tau)) \leqslant \delta_k'\ \forall \tau \in [0, \Delta_k)$ and if $\delta_k' < V_k(x_0) \leqslant c_k^{\max}$, then $\dot{V}_k(x(\tau)) \leqslant -\varepsilon_k^*\ \forall \tau \in [0, \Delta_k)$.

For the Lyapunov-based predictive control design, the control action at state x and time t is obtained by solving, on-line, a finite horizon optimal control problem of the form

$$P(x,t) : \min\{J(x,t,u_k(\cdot)) | u_k(\cdot) \in S_k\} \tag{6}$$

$$\text{s.t. } \dot{x} = f_k(x) + G_k(x)u_k \tag{7}$$

$$\dot{V}_k(x(\tau)) \leqslant -\varepsilon_k \quad \text{if} \quad V_k(x(t)) > \delta_k', \quad \tau \in [t, t+\Delta_k) \tag{8}$$

$$V_k(x(\tau)) \leqslant \delta_k' \quad \text{if} \quad V_k(x(t)) \leqslant \delta_k', \quad \tau \in [t, t+\Delta_k) \tag{9}$$

where ε_k, δ'_k are defined in Proposition 1, $S_k = S_k(t, T)$ is the family of piecewise continuous functions (functions continuous from the right), with period Δ_k, mapping $[t, t + T_k]$ into $\mathcal{U}_k$, T is the specified horizon and V_k is the Lyapunov function used in the bounded controller design. A control $u_k(\cdot)$ in S_k is characterized by the sequence $\{u_k[j]\}$ where $u_k[j] := u_k(j\Delta_k)$ and satisfies $u_k(t) = u_k[j]$ for all $t \in [j\Delta_k, (j+1)\Delta_k)$. The performance index is given by

$$J(x, t, u_k(\cdot)) = \int_t^{t+T} [\|x^u(s; x, t)\|^2_{Q_k} + \|u_k(s)\|^2_{R_k}]\, \mathrm{d}s \tag{10}$$

where Q_k, R_k are positive semi-definite, strictly positive definite, symmetric matrices, respectively, and $x^u(s; x, t)$ denotes the solution of Equation (1), due to control u_k, with initial state x at time t. The minimizing control $u^0_k(\cdot) \in S_k$ is then applied to the plant over the interval $[t, t + \Delta_k)$ and the procedure is repeated indefinitely. Stability properties of the closed-loop system under the Lyapunov-based predictive controller are inherited from the bounded controller under discrete implementation and are stated in Proposition 2 below (for a proof and more details, see Reference [22]).

Proposition 2

Consider the constrained system of Equation (1) for a fixed value of k with $\theta_k(t) = 0$ $\forall t \geqslant 0$ under the MPC control law of Equations (6)–(10), designed using a control Lyapunov function V_k that yields a stability region Ω_k under continuous implementation of the bounded controller of Equation (3) with a fixed $\rho_k > 0$. Then, given any positive real number d_k, there exist positive real numbers Δ^*_k and δ'_k, such that if $x(0) \in \Omega_k$ and $\Delta \in (0, \Delta^*_k]$, then $x(t) \in \Omega_k$ $\forall t \geqslant 0$ and $\limsup_{t\to\infty} \|x(t)\| \leqslant d_k$.

Remark 2

Note that Lyapunov-based predictive control approaches (see, for example, References [40, 41]) typically incorporate a similar Lyapunov function decay constraint, albeit requiring the constraint of Equation (8) to hold at the *end* of the prediction horizon as opposed to during the first time step, and assume the initial feasibility of this constraint. In contrast, the predictive controller formulation of Equations (6)–(10) requires that the value of the Lyapunov function decrease during the first step only, allowing for the use of the auxiliary controller to explicitly characterize the set of initial conditions starting from where the predictive controller is guaranteed to be feasible and stabilizing.

Remark 3

The fact that only practical stability is achieved is not a limitation of the MPC formulation, but is due to discrete implementation. Even if the bounded controller is used instead, under the same implement-and-hold time of Δ_k, the bounded controller can also only guarantee that the state of the closed-loop system converges to a neighbourhood of the origin the size of which is limited by the value of the hold time, Δ_k (in the limit as Δ_k goes to zero—continuous implementation—the bounded controller and the predictive controller enforces asymptotic stability). Note also, that any other Lyapunov-based nonlinear control design that provides an explicit characterization of the stability region, and is robust with respect to discrete implementation can be used as an auxiliary controller.

Remark 4

One of the key challenges that impact on the practical implementation of MPC is the inherent difficulty of characterizing, *a priori*, the set of initial conditions starting from where a given MPC controller is guaranteed to stabilize the closed-loop system, or for a given set of initial conditions, to identify the value of the prediction horizon for which the optimization problem will be feasible. Use of conservatively large horizon lengths to address stability only increases the size and complexity of the nonlinear optimization problem and could make it intractable. Owing to the fact that the closed-loop stability is guaranteed by the Lyapunov-based predictive controller from an explicitly characterized set of initial conditions, irrespective of the prediction horizon, the time required for the computation of the control action, if so desired, can be made smaller by reducing the size of the optimization problem by decreasing the prediction horizon.

3.2. Performance-based reconfiguration

The main idea behind the fault-tolerant control design is as follows: (1) use the presence of the state in the stability regions of the candidate control configurations to compute the set of suitable backup configurations, and (2) use the auxiliary Lyapunov-based nonlinear controller to estimate the 'cost' under each of the suitable control configurations, and choose the one with the minimum cost. To formalize this idea, consider the constrained nonlinear system of Equation (1) without uncertainty (i.e. $\theta_k(t) = 0 \ \forall t \geqslant 0$ and $\forall k = 1, \ldots, N$) for which the bounded controllers of the form of Equation (3) and Lyapunov-based predictive controllers of the form of Equations (6)–(9) have been designed and the stability regions Ω_j, $j = 1, \ldots, N$ under the Lyapunov-based predictive controllers have been explicitly characterized. Let $d_{\max} = \max_{j=1,\ldots,N} d_j$, where d_j was defined in proposition 1 and let $\Omega_U = \bigcup_{j=1}^{N} \Omega_j$. For a given control configuration, define $J_j(t) = \int_t^{t+T_j} [\|x^u(s; x, t)\|_Q^2 + \|b_k(s)\|_R^2]\, \mathrm{d}s$ where $t + T_j \geqslant t$ is the earliest time at which the state of the closed-loop system under the bounded controller enters the level set defined by $V_j(x) = \delta_j'$, and Q_j, R_j are the penalty matrices used in the predictive controller design. Theorem 1 below formalizes the result.

Theorem 1

Let $k(0) = i$ for some $i \in \mathscr{K}$ and $x(0) := x_0 \in \Omega_i$. Let T_i^f be the earliest time that a fault occurs. Furthermore, let $\mathscr{F} \in \mathscr{K} := \{j : j \neq i, x(T_i^f) \in \Omega_j\}$, and let l be such that $J_l = \min_{j \in F} J_j$ then the following switching rule:

$$k(t) = \left\{ \begin{array}{ll} i, & 0 \leqslant t < T_i^f \\ l, & t \geqslant T_i^f \end{array} \right\} \tag{11}$$

guarantees that $x(t) \in \Omega_U \ \forall t \geqslant 0$ and $\limsup_{t\to\infty} \|x(t)\| \leqslant d_{\max}$.

Proof of Theorem 1

We consider the two possible cases; first if no switching occurs, and second if a switch occurs at a time T_i^f.

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

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

Remark 5
The fault-tolerant controller is implemented as follows:

- Given the nonlinear process of Equation (1), identify the available control configurations $k = 1, \ldots, N$ and for each control configuration, design the controllers of Equation (3), and Equations (6)–(9) and calculate an estimate of the stability region $\Omega_k, \ k = 1, \ldots, N$.
- Given any $x_0 \in \Omega_i$, initialize the closed-loop system under the Lyapunov-based predictive controller of Equations (6)–(9).
- At any time T_i^f that a fault occurs, out of the available backup configurations ascertain the suitability of a candidate backup configuration $j \neq i$ (i.e. other than the current one) via checking whether or not the state of the closed-loop system resides in the stability region estimate under the candidate control configuration (i.e. to check if $x(T_i^f) \in \Omega_j$). If the state of the closed-loop system resides in the stability region of control configuration j, include its index in the set $\mathscr{F}$. For all the backup-configurations whose index is present in the set $\mathscr{F}$, compute the cost J_j, by running closed-loop simulations under the bounded controller of Equation (3), over a time by which the bounded controller drives the closed-loop state into the neighbourhood of the origin defined by the level set of $V_j(x) = \delta_j'$.
- Pick the control configuration that yields the lowest cost. Apply the Lyapunov-based predictive controller using this control configuration to achieve closed-loop stability.

Remark 6
Compared to References [31, 32], the fault-tolerant controller in the present work incorporates performance considerations in the switching logic as well as in computing the control action under the fall-back control configurations. In the event that the process state, at the time of the failure of the primary control configuration, lies in the stability region of more than one backup control configuration, the performance considerations expressed in the objective function are used in choosing which control configuration should be implemented in the closed-loop system. Note, however, that the receding horizon implementation of the predictive controller renders it unsuitable for evaluating on-line an estimate of the value of the objective function in driving the state from the current value to the equilibrium point (the cost-to-go). To this end, the auxiliary controller is used in estimating the control configuration that yields a lower cost; the practical justification behind doing this is that: (1) the Lyapunov-based predictive controller enforces the decay of the same Lyapunov function that is used in the auxiliary controller, and (2) the auxiliary controller provides an explicit control law, thus making it easier to estimate the 'cost-to-go' using fast simulations. In case that the cost-to-go can be computed using other computational techniques, these can be used within the proposed approach to pick the appropriate backup control configuration that yields the lowest cost. Either ways, once the cost has been estimated, the optimization problem in the switching logic involves only finding the minimum out of a set of numbers (costs), and picking out the index that corresponds to the minimum cost. Note also that if the state at the time of a failure lies outside the stability region

of all of the backup controllers, then this indicates that the backup controllers do not have enough control action available and calls for increasing the allowable control action in the fall-back configurations. Note that the set of initial conditions starting from where a given control configuration can stabilize a steady state—the so-called null-controllable region—is fundamentally limited by the constraints on the available control action, and that different control laws typically provide estimates of the stability region which are subsets of the null-controllable region.

3.3. Application to the chemical process example

For the chemical reactor example of Section 2.1, we first design the Lyapunov-based predictive controller and compute an estimate of the stability region under each control configuration using the auxiliary Lyapunov-based bounded controller. In the simulations, the constraints of Equations (8)–(9) are replaced by a constraint of the form $V_k(x(t+\Delta_k)) \leqslant V_k^b(x(t+\Delta_k))$ (with $\Delta_k = 0.02$ min) where $V_k^b(x(t+\Delta_k))$ is the predicted value of the Lyapunov function at $t+\Delta_k$ under the auxiliary controller. Note that once again the control action computed by the auxiliary controller provides a feasible solution to this constraint. Figure 2 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. The reactor under the first control configuration 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, and the supervisor proceeds to monitor the evolution of the closed-loop trajectory.

We first demonstrate the overriding stability considerations in the choice of the backup control configuration, i.e. a case where at the time of the failure of the primary control configuration, the state of the closed-loop system resides in the stability region of only one of the backup control configurations, and only a switch to that control configuration achieves closed-loop stability. As shown by the solid lines in Figures 2 and 3, the controller proceeds to drive the

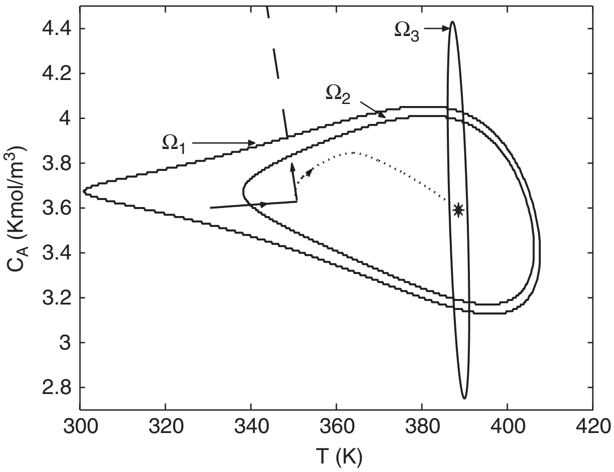

Figure 2. Evolution of closed-loop state profiles subject to failure in control configuration 1 (solid line) under the switching rule of Theorem 1 (dotted line) and under arbitrary switching (dashed line).

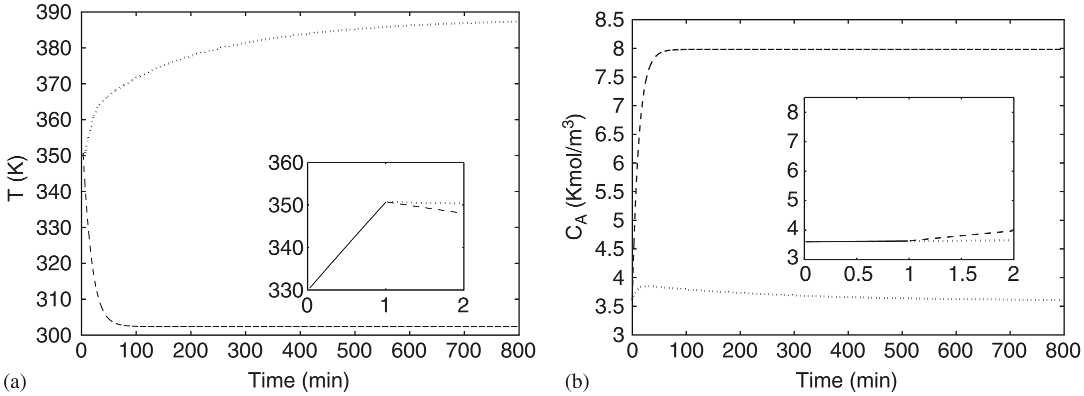

Figure 3. Evolution of closed-loop: (a) temperature; and (b) concentration subject to failure in control configuration 1 (solid lines) under the switching rule of Theorem 1 (dotted lines) and under arbitrary switching (dashed lines).

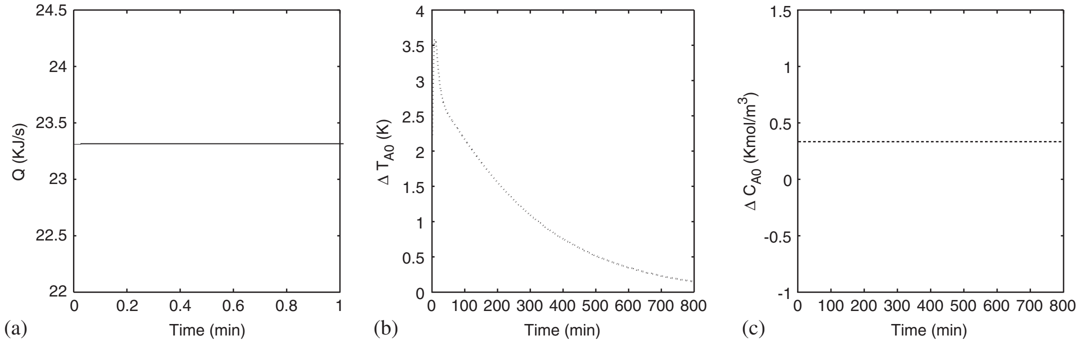

Figure 4. Manipulated input profiles under: (a) control configuration 1 (solid line); (b) control configuration 2 (under the switching rule of Theorem 1 (dotted line)); and (c) control configuration 3 (under arbitrary switching (dashed line)).

closed-loop trajectory towards the desired steady state, up until the Q-configuration fails after 1 min of reactor startup (see Figure 4(a)). If the supervisor switches arbitrarily, and in particular, switches to backup configuration 3, closed-loop stability is not achieved (dashed lines in Figures 2 and 3). Note that this happens because the closed-loop process state is outside the stability region of the third control configuration, and even though the third control configuration does not encounter a fault, the limited control action available in this configuration is unable to achieve closed-loop stability. From Figure 2, 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. Hence, on the basis of the switching logic of Equation (11), when the supervisor activates the second configuration (with T_{A0} as the manipulated input, see Figure 4(b)), the result is that upon switching to the T_{A0}-configuration, the corresponding controller stabilizes the closed-loop system.

We next demonstrate the scenario where performance considerations dictate the choice of the backup control configuration. To this end, consider the closed-loop system from the same initial condition as before under control configuration 1, but that control configuration 1 continues to be operating until 5.5 min, and at the time of the failure, the closed-loop state resides in the stability region of both the backup control configurations (see Figure 5). The auxiliary controllers are used to estimate the cost under the control configurations 2 and 3, and yield costs of 307.88 and 105.31, respectively. Using the switching rule, control configuration 3 is implemented in closed-loop system and stabilizes the closed-loop incurring a cost of 105.31. In contrast, if one were to use configuration 2, the cost incurred would be 276.94 which is lower than the estimate obtained using the auxiliary controller, yet more than the cost incurred under control configuration 3 (the corresponding state and input profiles are showed by dashed and dotted lines in Figures 6 and 7, respectively).

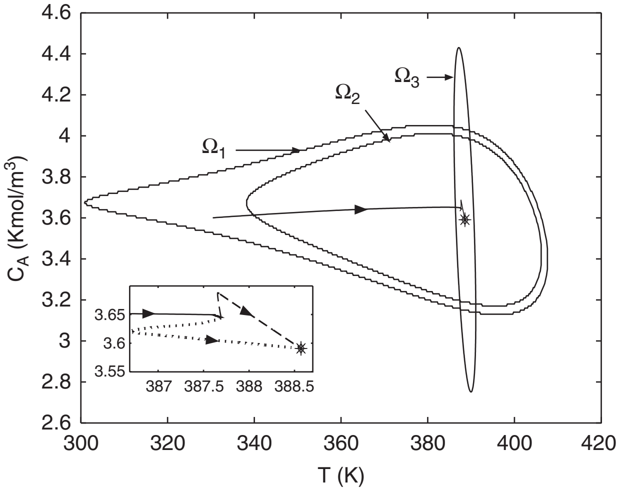

Figure 5. Evolution of closed-loop state profiles subject to failure in control configuration 1 (solid line) and switching to configuration 2 (dotted line) and, according to the switching rule of Theorem 1, to configuration 3 (dashed line).

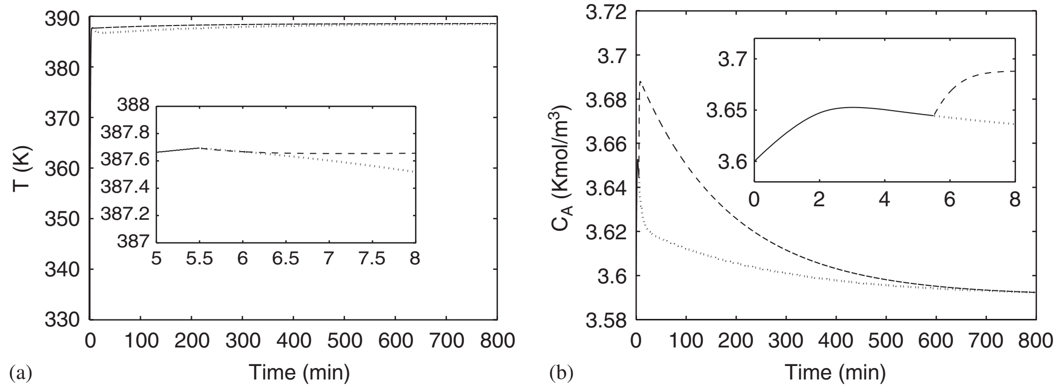

Figure 6. Evolution of closed-loop: (a) temperature; and (b) concentration subject to failure in control configuration 1 (solid line) and switching to configuration 2 (dotted lines) and, according to the switching rule of Theorem 1, to configuration 3 (dashed lines).

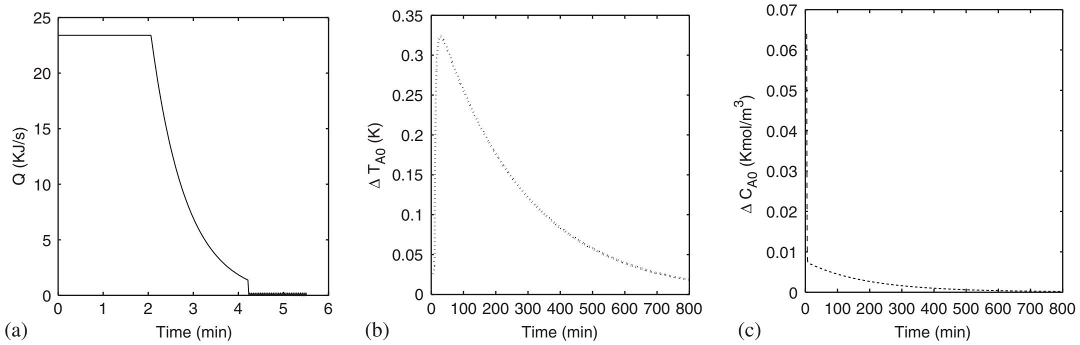

Figure 7. Manipulated input profiles under: (a) control configuration 1 (solid line); (b) control configuration 2 (dotted lines); and (c) according to the switching rule of Theorem 1 to control configuration 3 (dashed lines).

4. FAULT-TOLERANT CONTROL: ROBUSTNESS CONSIDERATIONS

In this section, we consider the problem of incorporating robustness into the fault-tolerant control method. Note that in the presence of uncertainty, the feasibility guarantees of the predictive controller of Equations (6)–(9) may no longer hold, or it may happen that the predictive controller is feasible but not stabilizing (enforcing negative-definiteness of $\dot{V}$ *without* accounting for the uncertainty does not imply that $\dot{V} < 0$ in the presence of uncertainty). Preparatory to its use within the robust fault-tolerant controller (to be proposed in Section 4.2), we review a robust hybrid predictive controller that provides an explicit characterization of the stability region in the presence of uncertainty and input constraints.

4.1. Robust hybrid predictive controller

In this section, we employ switching between the bounded robust controller of Equation (3) and the representative predictive controller of Equation (5), to provide the switched (the switching here is between control algorithms, and not control configurations) closed-loop system with an explicit characterization of the closed-loop stability region. To this end, we first cast the system of Equation (1), for a fixed value of k (i.e. under a given control configuration) as a switched system of the form:

$$\dot{x} = f(x) + G_k(x)u_k^j + W_k(x)\theta_k(t), \quad \|u_k^j\| \leqslant u_k^{\max} \tag{12}$$

where $j : [0, \infty) \rightarrow \{1, 2\}$ is the switching signal which is assumed to be a piecewise continuous (from the right) function of time, implying that only a finite number of switches between the two controllers is allowed on any finite-time interval. The index, $j(t)$, represents a discrete state that indexes the control input, u_k, with the understanding that $j(t) = 1$ if and only if MPC is used and $j(t) = 2$ if and only if bounded control is used. Theorem 2 below presents the robust hybrid predictive controller (for the proof and more details, see Reference [21]).

Theorem 2

Consider the switched nonlinear system of Equation (12), the model predictive controller of Equation (5) and the bounded controller of Equation (3). Let $x(0) = x_0 \in \Omega_k$, and initially set $T_k^s = T_k^D = T_k^{\text{inf}} = \infty$. At the earliest time $t \geqslant 0$ for which the closed-loop state under MPC satisfies $V_k(x(t^-)) = c_k^{\max}$ set $T_k^s = t$. At the earliest time for which the closed-loop state under MPC satisfies $\|x(t)\| \leqslant d_k^r$ where d_k^r was defined in Equation (4), set $T_k^D = t$. Finally, at the earliest time t that MPC is infeasible, set $T_k^{\text{inf}} = t$. Define $T_k^{\text{switch}} = \min\{T_k^s, T_k^D, T_k^{\text{design}}, T_k^{\text{inf}}\}$, where $0 \leqslant T_k^{\text{design}} < \infty$ is arbitrary. Then, the switching rule

$$j(t) = \left\{ \begin{array}{ll} 1, & 0 \leqslant t < T_k^{\text{switch}} \\ 2, & t \geqslant T_k^{\text{switch}} \end{array} \right\} \tag{13}$$

guarantees that $x(t) \in \Omega_k \ \forall t \geqslant 0$ and $\limsup_{t\to\infty} \|x(t)\| \leqslant d_k^r$.

Remark 7

The robust hybrid predictive controller of Theorem 1 is designed and implemented to achieve closed-loop stability using a control configuration k as follows:

- Given the nonlinear system of Equation (12), θ_k^b and $u_k^{\max}$, design the bounded robust controller of Equation (3), and calculate an estimate of its stability region Ω_k for the control configuration k.
- Design/pick an MPC formulation (the MPC formulation could be min–max optimization based, linear or nonlinear, and with or without stability constraints). For convenience, we refer to the general MPC formulation of Equation (5).
- Given any $x_0 \in \Omega_k$, check the feasibility of the optimization problem in Equation (5) at $t = 0$, and if feasible, start implementing MPC.
- If at any time, MPC becomes infeasible ($t = T_k^{\text{inf}}$), or the states of the closed-loop system approach the boundary of Ω_k ($t = T_k^s$), or the closed-loop states enter the set $\mathbb{D}_k^r$ ($t = T_k^D$) then switch to the bounded controller, else keep MPC active in the closed-loop system until a time T^{design}.
- Switch to the bounded robust controller at T_k^s, T_k^D, T_k^{design}, or T_k^{inf}, whichever comes earliest, to achieve practical closed-loop stability under the kth control configuration.

Remark 8

The purpose of switching to the bounded robust controller after the time T_k^{design} is to ensure convergence to $\mathbb{D}_k^r$ and avoid possible cases where the closed-loop states, under MPC, could wander inside Ω_k without actually converging to, and staying within, $\mathbb{D}_k^r$. Convergence to $\mathbb{D}_k^r$ could also be achieved (see, for example, References [18, 20]), by switching to the bounded controller when $\dot{V}_k \geqslant 0$ under MPC. However, in the presence of uncertainty, such a condition might be very restrictive in the sense that it may terminate MPC implementation too early. Note that if an MPC design is used that guarantees robust stability for the uncertain nonlinear system if initially feasible, it could be implemented for all time (T_k^{design} can be chosen to be practically infinity) to stabilize the closed-loop system. The stability safeguards, provided by the bounded controller, are still required because the stability of any MPC formulation, robust or otherwise, is based on the assumption of initial feasibility, which cannot be verified short of testing, via simulation, an initial condition for feasibility.

Remark 9

We note that while the MPC framework provides a transparent way of specifying a performance objectives, the various MPC formulations, in general, may not be optimal, and only approximate the infinite horizon optimal cost to varying degrees of success. The choice of a particular MPC design can be made entirely on the basis of the desired tradeoff between performance and computational complexity because the stability guarantees of the robust hybrid predictive controller are independent of the specific MPC formulation being used.

4.2. *Robust fault-tolerant control*

The robust fault-tolerant controller is implemented as follows:

1. Given the nonlinear process of Equation (1), identify the available control configurations $k = 1, \dots, N$ and for each control configuration, design the robust hybrid predictive controllers of Theorem 2 and calculate an estimate of the stability region Ω_k, $k = 1, \dots, N$.
2. Given any $x_0 \in \Omega_k$, initialize the closed-loop system under the robust hybrid predictive controller of Theorem 2.
3. At any time T_1^f that a fault occurs, implement the control configuration j for which the closed-loop state resides in its stability regions estimate (Ω_j) to achieve closed-loop stability.

Remark 10

Note that robustness considerations are incorporated in the controller design (use of robust hybrid predictive controllers) and also in characterizing the stability region. Performance considerations can be incorporated in the switching rule in a similar fashion as in the previous section, and in the design of controllers via use of robust predictive control designs as a component of the robust hybrid predictive controllers (for a demonstration, see the simulation example below).

4.3. *Application to the chemical process example with uncertainty and disturbance*

In this section, we consider once again the motivating example of Section 2.1, albeit with uncertainty and disturbances. In particular, we consider parametric uncertainty in the heat of reactions, and in particular a 50% uncertainty in the heats of reactions, i.e. $\theta_i(t) = 0.5(-\Delta H_{i,\mathrm{nom}})$, $i = 1, \dots, 3$, and disturbance in the inlet feed temperature, simulated by $\theta_4(t) = 0.5 T_{A0s} \sin t$. Figure 8 depicts the stability region computed using the bounded robust controller with $\rho = 0.0001$, $\phi = 0.0001$, $\chi = 1.0001$, in the (T, C_A) space, for the control configurations using Q as the manipulated input variable and using T_{A0} as the manipulated input variable. The desired steady state is depicted with an asterisk that lies in the intersection of the two stability regions (note the reduction in the estimate of the stability region as a result of accounting for the presence of uncertainty).

The hybrid predictive control structure allows for the use of any predictive controller formulation, while still guaranteeing stability from an explicitly characterized set of initial conditions. Within the hybrid predictive controller, we use a modification of the Lyapunov-based predictive controller of Section 3.1. In particular, for the predictive control design, the

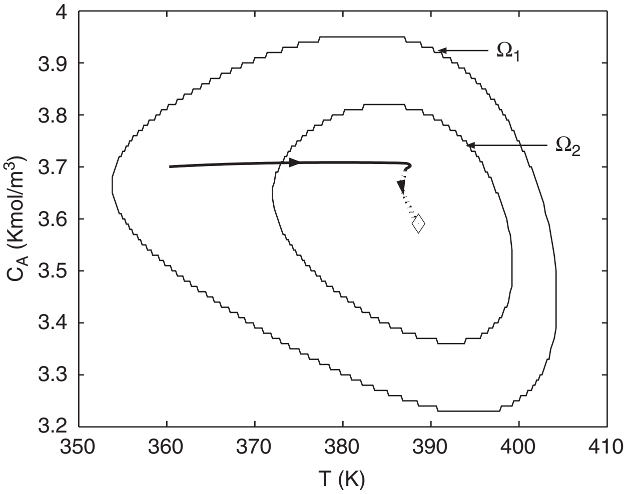

Figure 8. Evolution of closed-loop state profiles under the switching rule of Section 4.2 subject to failure in control system 1.

control action at state x and time t is obtained by solving, on-line, a finite horizon optimal control problem of the form

$$P(x,t) : \min\{J(x,t,u_k(\cdot)) | u_k(\cdot) \in S_k, \theta_k(t) = \theta_0 \in \Theta_k\} \tag{14}$$

$$\text{s.t. } \dot{x} = f_k(x) + G_k(x)u_k + W_k(x)\theta_k(t) \tag{15}$$

$$V_k(x(t+\Delta_k)) \leqslant V_k^b(x(t+\Delta_k)) \tag{16}$$

where $V_k^b(x(t+\Delta_k))$ is the predicted value of the Lyapunov function at $t+\Delta$ under the robust bounded controller with $\theta_k(t) = \theta_0 \in \Theta_k$, $S_k = S_k(t,T)$ is the family of piecewise continuous functions (functions continuous from the right), with period Δ_k, mapping $[t, t+T_k]$ into $\mathcal{U}_k$, T_k is the specified horizon and V_k is the Lyapunov function used in the bounded controller design. The performance index is given by

$$J(x,t,u_k(\cdot),\theta_0) = \int_t^{t+T_k} [\|x^u(s;x,t)\|_{Q_k}^2 + \|u_k(s)\|_{R_k}^2]\, ds \tag{17}$$

where Q_k, R_k are positive semi-definite, strictly positive definite, symmetric matrices, respectively, and $x^u(s;x,t)$ denotes the solution of Equation (1), due to control u_k under a fixed value of uncertainty $\theta_k(t) = \theta_0$, with initial state x at time t. The minimizing control $u_k^0(\cdot) \in S_k$ is then applied to the plant over the interval $[t, t+\Delta_k)$ and the procedure is repeated indefinitely.

Note that as in the case without uncertainty, initial feasibility of the optimization problem of Equations (14)–(17) is guaranteed for all initial conditions within the stability region of the bounded robust controller. There is no guarantee, however, that the control action computed by the predictive controller will lead to a decay in the value of the Lyapunov function; this is so because the control action is computed by using only a fixed value of the uncertainty, and is not computed to ensure the satisfaction of the Lyapunov-function decay constraint for all possible realizations of the uncertainty, as is customarily done in robust predictive control approaches. The modification used in the simulation example, however, while not providing rigorous robust stability guarantees, incorporates some robustness consideration in the Lyapunov-based predictive controller without making the computation intractable by requiring min–max computations.

The reactor under the first control configuration is initialized at $T(0) = 360$ K, $C_A(0) = 3.7\ \mathrm{kmol/m^3}$, $C_B(0) = 0.0\ \mathrm{kmol/m^3}$, using the Q-control configuration, under the hybrid predictive controller for configuration 1 (with $T^{\mathrm{design}} = 100$ min) and the supervisor proceeds to monitor the evolution of the closed-loop trajectory. As shown by the solid lines in Figures 8

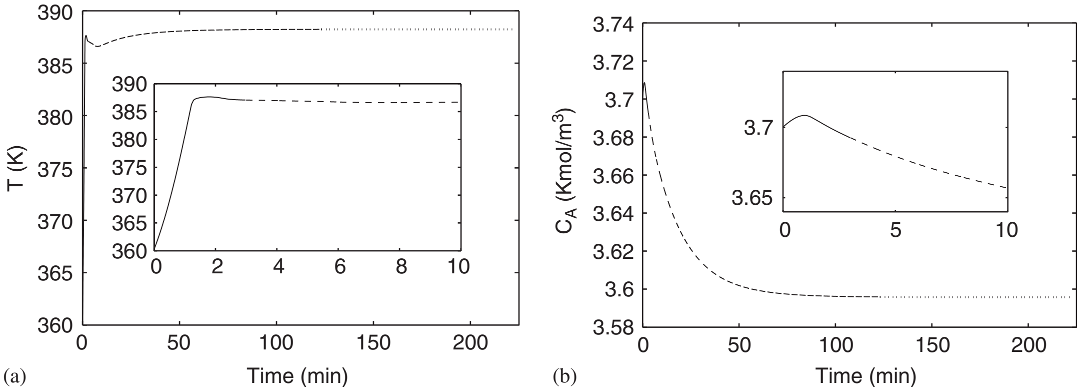

Figure 9. Evolution of closed-loop: (a) temperature; and (b) concentration under the switching rule of Section 4.2 subject to failure in control system 1.

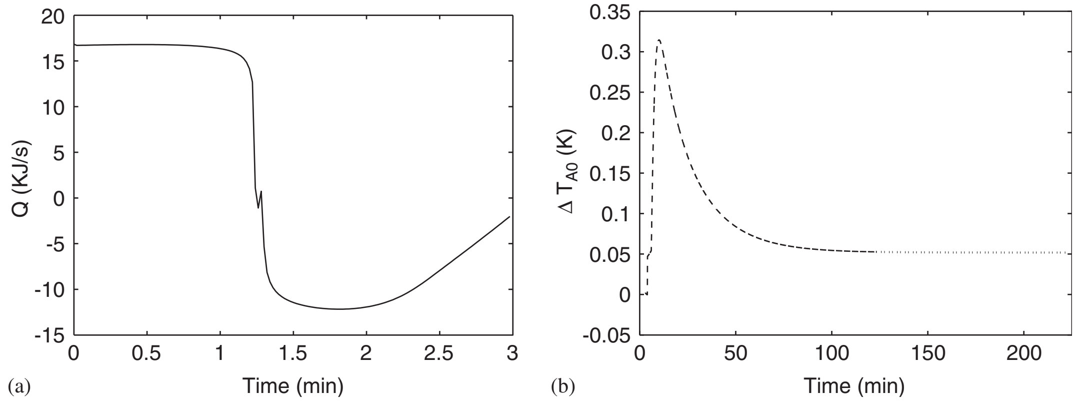

Figure 10. Manipulated input profiles under: (a) control configuration 1; and (b) control configuration 2 under the switching rule of Section 4.2 subject to failure in control system 1.

and 9, the controller proceeds to drive the closed-loop trajectory towards the desired steady state, up until the Q-configuration fails after 3 min of reactor startup (see Figure 10(a)). Until this time, only the predictive controller component of the robust hybrid predictive controller is used for the first control configuration. From Figure 8, 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. Hence, on the basis of the switching algorithm of Section 4.2, when the supervisor activates the second configuration (with T_{A0} as the manipulated input, see Figure 10(b)), the result is that upon switching to the T_{A0}-configuration, the corresponding robust hybrid predictive controller stabilizes the closed-loop system. Note also that in operating the second control configuration, the robust Lyapunov-based predictive controller is able to drive the state trajectory sufficiently close to the origin, and the robust bounded controller is used only toward the end to drive the state trajectory into the desired neighbourhood of the origin.

5. CONCLUDING REMARKS

This work considered the problem of control system/actuator failures in nonlinear processes subject to input constraints and presented two approaches for fault-tolerant control that focussed on incorporating performance and robustness considerations, respectively. Performance considerations were incorporated in the design of the controllers (via the use of predictive control approach) as well as in the reconfiguration logic to achieve fault-tolerant control. To handle the problem of uncertainty, robust hybrid predictive controllers were designed for the individual control configurations. The application of the fault-tolerant control methods incorporating performance and robustness considerations was demonstrated via a benchmark chemical reactor example.

REFERENCES

1. Yang GH, Wang JL, Soh YC. Reliable H_∞ control design for linear systems. *Automatica* 2001; **37**:717–725.
2. Patton RJ. Fault-tolerant control systems: the 1997 situation. *Proceedings of the IFAC Symposium SAFEPROCESS 1997*, Hull, U.K., 1997; 1033–1054.
3. Zhou DH, Frank PM. Fault diagnostics and fault tolerant control. *IEEE Transactions on Aerospace and Electronic Systems* 1998; **34**:420–427.
4. Bao J, Zhang WZ, Lee PL. Decentralized fault-tolerant control system design for unstable processes. *Chemical Engineering Science* 2003; **58**:5045–5054.
5. Wu NE. Coverage in fault-tolerant control. *Automatica* 2004; **40**:537–548.
6. Bequette WB. Nonlinear control of chemical processes: a review. *Industrial and Engineering Chemistry Research* 1991; **30**:1391–1413.
7. Ydstie EB. Certainty equivalence adaptive control: paradigms puzzles and switching. *Proceedings of 5th International Conference on Chemical Process Control*, Tahoe City, CA, 1997; 9–23.
8. Christofides PD, El-Farra NH. *Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-Delays*. Springer: New York, 2005.
9. Garcia CE, Prett DM, Morari M. Model predictive control—theory and practice—a survey. *Automatica* 1989; **25**:335–348.
10. Mayne DQ, Rawlings JB, Rao CV, Scokaert POM. Constrained model predictive control: stability and optimality. *Automatica* 2000; **36**:789–814.
11. Lin Y, Sontag ED. A universal formula for stabilization with bounded controls. *Systems and Control Letters* 1991; **16**:393–397.
12. Teel AR. Global stabilization and restricted tracking for multiple integrators with bounded controls. *Systems and Control Letters* 1992; **18**:165–171.

13. Kapoor N, Daoutidis P. Stabilization of systems with input constraints. *International Journal of Control* 1998; **34**:653–675.
14. Kokotovic PV, Arcak M. Constructive nonlinear control: a historical perspective. *Automatica* 2001; **37**:637–662.
15. El-Farra NH, Christofides PD. Integrating robustness, optimality and constraints in control of nonlinear processes. *Chemical Engineering Science* 2001; **56**:1841–1868.
16. El-Farra NH, Armaou A, Christofides PD. Analysis and control of parabolic PDE systems with input constraints. *Automatica* 2003; **39**:715–725.
17. El-Farra NH, Christofides PD. Bounded robust control of constrained multivariable nonlinear processes. *Chemical Engineering Science* 2003; **58**:3025–3047.
18. El-Farra NH, Mhaskar P, Christofides PD. Uniting bounded control and MPC for stabilization of constrained linear systems. *Automatica* 2004; **40**:101–110.
19. Mhaskar P, El-Farra NH, Christofides PD. Hybrid predictive control of process systems. *AIChE Journal* 2004; **50**:1242–1259.
20. El-Farra NH, Mhaskar P, Christofides PD. Hybrid predictive control of nonlinear systems: method and applications to chemical processes. *International Journal of Robust and Nonlinear Control* 2004; **14**:199–225.
21. Mhaskar P, El-Farra NH, Christofides PD. Robust hybrid predictive control of nonlinear systems. *Automatica* 2005; **41**:209–217.
22. 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.
23. Mhaskar P, El-Farra NH, Christofides PD. Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. *Systems and Control Letters* 2006, in press.
24. Grossmann IE, van den Heever SA, Harjukoski I. Discrete optimization methods and their role in the integration of planning and scheduling. *Proceedings of 6th International Conference on Chemical Process Control*, Tucson, AZ, 2001; 124–152.
25. Garcia-Onorio V, Ydstie BE. Distributed, asynchronous and hybrid simulation of process networks using recording controllers. *International Journal of Robust and Nonlinear Control* 2004; **14**:227–248.
26. Hespanha JP, Morse AS. Stability of switched systems with average dwell time. *Proceedings of 38th IEEE Conference on Decision and Control*, Phoenix, AZ, 1999; 2655–2660.
27. DeCarlo RA, Branicky MS, Pettersson S, Lennartson B. Perspectives and results on the stability and stabilizability of hybrid systems. *Proceedings of the IEEE* 2000; **88**:1069–1082.
28. Bemporad A, Morari M. Robust model predictive control: a survey. In *Robustness in Identification and Control*, Garulli A, Tesi A, Vicino A (eds), Lecture Notes in Control and Information Sciences, vol. 245. Springer: Berlin, 1999; 207–266.
29. El-Farra NH, Christofides PD. Coordinated feedback and switching for control of hybrid nonlinear processes. *AIChE Journal* 2003; **49**:2079–2098.
30. El-Farra NH, Mhaskar P, Christofides PD. Output feedback control of switched nonlinear systems using multiple Lyapunov functions. *Systems and Control Letters* 2005; **54**:1163–1182.
31. El-Farra NH, Gani A, Christofides PD. Fault-tolerant control of process systems using communication networks. *AIChE Journal* 2005; **51**:1665–1682.
32. Mhaskar P, Gani A, El-Farra NH, Christofides PD, Davis JF. Integrated fault-detection and fault-tolerant control for process systems. *AIChE Journal*, submitted.
33. Freeman RA, Kokotovic PV. *Robust Nonlinear Control Design*: *State-Space and Lyapunov Techniques*. Birkhauser: Boston, 1996.
34. Krstic N, Kanellakopoulos I, Kokotovic P. *Nonlinear and Adaptive Control Design* (1st edn). Wiley: New York, 1995.
35. Dubljevic S, Kazantzis N. A new Lyapunov design approach for nonlinear systems based on Zubov's method. *Automatica* 2002; **38**:1999–2007.
36. Grizzle JW, Kokotovic PV. Feedback linearization of sampled-data systems. *IEEE Transactions on Automatic Control* 1988; **33**:857–859.
37. Nesic D, Teel AR, Kokotovic PV. Sufficient conditions for stabilization of sampled-data nonlinear systems via discrete-time approximations. *Systems and Control Letters* 1999; **38**:259–270.
38. Kazantzis N. A functional equations approach to nonlinear discrete-time feedback stabilization through pole-placement. *Systems and Control Letters* 2001; **43**:361–369.
39. Zaccarian L, Teel AR, Nesic D. On finite gain L_P stability of nonlinear sampled-data systems. *Systems and Control Letters* 2003; **49**:201–212.
40. Kothare SLD, Morari M. Contractive model predictive control for constrained nonlinear systems. *IEEE Transactions on Automatic Control* 2000; **45**:1053–1071.
41. Primbs JA, Nevistic V, Doyle JC. A receding horizon generalization of pointwise min-norm controllers. *IEEE Transactions on Automatic Control* 2000; **45**:898–909.