2008 American Control Conference
Westin Seattle Hotel, Seattle, Washington, USA
June 11-13, 2008

Safe-Parking of Nonlinear Process Systems *

Rahul Gandhi and Prashant Mhaskar†
Department of Chemical Engineering
McMaster University
Hamilton, ON L8S 4L7, Canada

Abstract— **This work considers the problem of control of nonlinear process systems subject to input constraints and actuator faults. Faults are considered that preclude the possibility of continued operating at the nominal equilibrium point and a framework (which we call the safe-parking framework) is developed to enable efficient resumption of nominal operation upon fault-recovery. First Lyapunov-based model predictive controllers, that allow for an explicit characterization of the stability region subject to constraints on the manipulated input, are designed. The stability region characterization is utilized in selecting 'safe-park' points from the safe-park candidates (equilibrium points subject to failed actuators). Specifically, a candidate parking point is termed a safe-park point if 1) the process state at the time of failure resides in the stability region of the safe-park candidate (subject to depleted control action), and 2) the safe-park candidate resides within the stability region of the nominal control configuration. Performance considerations, such as ease of transition from and to the safe-park point and cost of running the process at the safe-park point, are quantified and utilized in choosing the optimal safe-park point. The proposed framework is illustrated using a chemical reactor example.**

Key words: Fault Tolerant Control, Safe-parking, Constraints, Nonlinear Process Systems

I. Introduction

Chemical process operation and control involves accounting for process complexity (manifested as nonlinearities), operational issues (such as constraints and disturbances), as well as eventualities, such as faults. Smooth operation of chemical processes, therefore, relies on adequate design and maintenance, appropriate monitoring systems to detect and diagnose eventualities, and the presence of correcting mechanisms that, having been 'informed' of an eventuality, prevent or minimize loss of performance, shutdowns, or hazardous situations. The ubiquitous nature of faults, and the extensive economic damage that results from faults (it is estimated that the U.S. petrochemical industry loses and estimated $20 billion per year due to faults; see, e.g., [1] and the reference therein) has motivated extensive research on development of strategies for handling faults.

The existing methods for handling faults assume availability of sufficient residual control effort or redundant control configurations to preserve operation at the nominal equilibrium point, and can be categorized within the robust/reliable, and reconfiguration-based fault-tolerant control approaches. Robust/reliable control approaches (e.g., see [2]) essentially rely on the robustness of the active control configuration to handle faults as disturbances. Several faults, however, cause significant erosion of the control effort in the active control configuration, and closed-loop stability cannot be preserved by simply re-tuning the controller in the active control configuration. If redundant control configurations are available, control–loop reconfiguration (activating an appropriately chosen fall-back configuration) can be implemented to preserve closed–loop stability at the nominal equilibrium point.

In determining the suitability of a backup control configuration, the presence of constraints, nonlinearity and uncertainty, as well as the switched nature of the closed–loop system (due to the switching between the control configurations) must be accounted for. The extensive research on control of nonlinear and switched systems (see, e.g., [3], [4], [5], [6], [7], [8], [9], [10]) has made available a number of tools that can be utilized to this end. These include Lyapunov-based nonlinear control designs (see, e.g., [3], [11] for a review, see [10]) that provide an explicit characterization of the stability region in the presence of constraints as well as model predictive control designs (see, for example the survey paper, [6]) that allow incorporation of performance considerations in the control design and provide stability guarantees based on the assumption of initial feasibility of the optimization problem. Recently, model predictive controllers have been designed [8], [9] that allow explicit characterization of the stability region in the presence of constraints, without assuming initial feasibility of the optimization problem. Several research efforts have also focussed on the problem of control of switched systems verifying [12] and enabling [8] closed–loop stability for a prescribed switching schedule.

The control tools described above have been utilized within reconfiguration-based fault-tolerant control structures focusing on closed–loop stability and performance, while accounting for process nonlinearity and constraints (see, e.g., [13], [14], [15]). Specifically, closed–loop stability is preserved (having first detected and isolated the occurrence of a fault) via implementing a backup control configuration chosen such that 1) the state at the time of the failure resides in the stability region of the candidate backup control configuration and 2) the backup configuration does not use the failed control actuator. However, all the reconfiguration-based fault-tolerant control designs of [14], [13], [15] assume the existence of a backup, redundant control configuration. The scenario where a fault results in temporary

*Financial support by NSERC and McMaster Advanced Control Consortium is gratefully acknowledged.

†Corresponding author: mhaskar@mcmaster.ca

loss of stability that cannot be handled by redundant control loops has not been explicitly addressed. In the absence of a framework for handling such faults, ad-hoc approaches could result in temporarily shutting down the process which can have substantially negative economic ramifications.

Motivated by the above considerations, this work considers the problem of control of nonlinear process systems subject to input constraints and destabilizing faults in the control actuators. Specifically, faults are considered that cannot be handled via robust control approaches or activation of redundant control configurations, and necessitate fault-rectification. A safe-parking framework is developed to determine how to run the process during fault-rectification to enable smooth resumption of nominal operation. The rest of the manuscript is organized as follows: we first present, in Section II-A, the class of processes considered, and review a Lyapunov-based predictive controller in Section II-B. The safe-parking problem is formulated in Section III-A, and Sections III-B and III-C, respectively. A chemical reactor example is used to illustrate the details of the safe-parking framework in Section III-D.

II. Preliminaries

In this section, we describe the class of processes considered and a Lyapunov-based model predictive control design.

A. Process description

We consider nonlinear process systems subject to input constraints and failures described by:

$$\dot{x}(t) \quad = \quad f(x(t)) + G(x(t))u_\sigma(t), u_\sigma(\cdot) \in \mathbf{U} \qquad (1)$$

where $x \in \mathbb{R}^n$ denotes the vector of state variables, $u_\sigma(t) \in \mathbb{R}^m$ denotes the vector of constrained manipulated inputs, taking values in a nonempty convex subset $\mathbf{U}$ of $\mathbb{R}^m$, where $\mathbf{U} = \{u \in \mathbb{R}^m : u_{min} \leq u \leq u_{max}\}$, where $u_{min}, u_{max} \in \mathbb{R}^m$ denote the constraints on the manipulated inputs, $f(0) = 0$ and $\sigma \in \{1, 2\}$ is a discrete variable that indexes the fault-free and faulty operation ($\sigma = 1$ denotes fault-free operation and $\sigma = 2$ denotes faulty operation). The vector function $f(x)$ and the matrix $G(x) = [g^1(x) \cdots g^m(x)]$ where $g^i(x) \in \mathbb{R}^n$, $i = 1 \cdots m$ are assumed to be sufficiently smooth on their domains of definition. The notation $\|\cdot\|_Q$ refers to the weighted norm, defined by $\|x\|_Q^2 = x'Qx$ for all $x \in \mathbb{R}^n$, where Q is a positive definite symmetric matrix 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 $f(\cdot)$. Throughout the manuscript, we assume that for any $u \in \mathbf{U}$ the solution of the system of Eq.1 exists and is continuous for all t, and we focus on the state feedback problem where $x(t)$ is assumed to be available for all t.

B. Lyapunov-based model predictive control

In this section, we briefly review a recent result on the design of a Lyapunov-based predictive controller that possesses an explicitly characterized set of initial conditions from where it is guaranteed to be feasible, and hence stabilizing in the presence of input constraints. Consider the system of Eq.1, for $\sigma(t) = 1$, under the predictive controller [8] of the form:

$$u_1(\cdot) \quad = \quad argmin\{J(x, t, u(\cdot))|u(\cdot) \in S\} \qquad (2)$$

$$s.t. \ \dot{x} \quad = \quad f(x) + G(x)u(t) \qquad (3)$$

$$\dot{V}(x(\tau)) \leq -\epsilon^* \ \ \forall \ \tau \in [t, t + \Delta) \ if \ \ V(x(t)) > \delta^{'} \qquad (4)$$

$$V(x(\tau)) \leq \delta^{'} \ \forall \ \tau \in [t, t + \Delta) \ \ if \ \ V(x(t)) \leq \delta^{'} \qquad (5)$$

where $S = S(t, T)$ is the family of piecewise continuous functions (functions continuous from the right), with period Δ, mapping $[t, t+T]$ into U and T is the horizon. Eq.3 is the nonlinear model describing the time evolution of the state x, V is a control Lyapunov function and $\delta^{'}$, ϵ^* are parameters to be determined. A control $u(\cdot)$ in S is characterized by the sequence $\{u[j]\}$ where $u[j] := u(j\Delta)$ and satisfies $u(t + \tau) = u[j]$ for all $\tau \in [t+j\Delta, t+(j+1)\Delta)$. The performance index is given by

$$J(x, t, u(\cdot)) = \int_t^{t+T} \left[\|x^u(s; x, t)\|_{Q_w}^2 + \|u(s)\|_{R_w}^2\right] ds \qquad (6)$$

where Q_w is a positive semi-definite symmetric matrix and R_w is a strictly positive definite symmetric matrix. $x^u(s; x, t)$ denotes the solution of Eq.1, due to control u, with initial state x at time t. The minimizing control $u[1] \in S$ is then applied to the plant over the interval $[t, t + \Delta)$ and the procedure is repeated indefinitely.

The stability properties of the predictive controller are characterized using a bounded controller [3], [11], for which one can show, using a standard Lyapunov argument, that whenever the closed–loop state, x, evolves within the region described by the set:

$$\Pi = \{x \in \mathbb{R}^n : L_f V(x) \leq u^{norm} \|(L_G V)'(x)\|\} \qquad (7)$$

where $u^{norm} > 0$ is such that $\|u\| \leq u^{norm}$ implies $u \in \mathbf{U}$, where $\|(\cdot)\|$ denotes the Euclidean norm of a vector, then the control law satisfies the input constraints, and the time-derivative of the Lyapunov function is negative-definite. An estimate of the stability region can be constructed using a level set of V, i.e.,

$$\Omega \quad = \quad \{x \in \mathbb{R}^n : V(x) \leq c^{max}\} \qquad (8)$$

where $c^{max} > 0$ is the largest number for which $\Omega \subseteq \Pi$. Closed–loop stability and feasibility properties of the closed–loop system under the Lyapunov–based predictive controller are inherited from the bounded controller under discrete implementation and are formalized in Theorem 1 below (for a proof, see [8]).

Theorem 1 [8]: *Consider the constrained system of Eq.1 under the MPC law of Eqs.2–6. Then, given any $d \geq 0$, $x_0 \in \Omega$, where Ω was defined in Eq.8, there exist positive real numbers $\delta^{'}$, ϵ^*, Δ^*, such that if $\Delta \in (0, \Delta^*]$, then the optimization problem of Eq.2-6 is feasible for all times, $x(t) \in \Omega$ for all $t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d$.*

Remark 1: The predictive controller formulation of Eqs.2–6 requires that the value of the Lyapunov function decrease during the first step only. Practical stability of the closed–loop system is achieved since only the first move of the set

of calculated moves is implemented and the problem is resolved at the next time step. If the optimization problem is initially feasible and continues to be feasible, then every control move that is implemented enforces a decay in the value of the Lyapunov function, leading to stability. Furthermore, the constraint of Eq.4 is guaranteed to be satisfied since the control action computed by the bounded controller design provides a feasible initial guess to the optimization problem. Finally, since the state is initialized in Ω, which is a level set of V, the closed–loop system evolves so as to stay within Ω, thereby guaranteeing feasibility at future times. The key idea in the predictive control design is to identify stability constraints that can a) be shown to be feasible and b) upon being feasible can guarantee stability. Note that the model predictive controller of Eqs.2–6 is only used to illustrate the safe-parking framework, and any other controller that provides an explicit characterization of the closed–loop stability region can be used within the proposed framework. With respect to the design of the Lyapunov-based predictive controller of Eqs.2–6, we also note that while the use of a control Lyapunov function provides a better estimate of the stability region, even a quadratic Lyapunov function (chosen such that it is locally a control Lyapunov function) can be used to generate (possibly conservative) estimates of the stability region. For further discussion on this issue, see [16].

III. Safe-parking of nonlinear process systems

We first formalize the problem in Section III-A, and present a safe-parking algorithm focusing on closed–loop stability in Section III-B. We incorporate performance considerations in the safe-parking framework in Section III-C.

A. Problem definition

We consider faults where one of the control actuators fails and reverts to the fail-safe value. Examples of fail-safe positions include fully open for a valve controlling a coolant flow rate, fully closed for a valve controlling a steam flow etc. Specifically, we characterize the fault occurring w.l.o.g., in the first control actuator at a time T^{fault}, subsequently rectified at a time $T^{recovery}$ (i.e., for $t \leq T^{fault}$ and $t > T^{recovery}$, $\sigma(t) = 1$ and $\sigma(t) = 2$ for $T^{fault} < t \leq T^{recovery}$), as $u_2^1(t) = u_{failed}^1$, with $u_{min}^1 \leq u_{failed}^1 \leq u_{max}^1$, where u^i denotes the ith component of a vector u, for all $T^{fault} < t \leq T^{recovery}$, leaving only u_2^i, $i = 2 \dots m$ available for feedback control. With $u_2^1(t) = u_{failed}^1$, there exists a (possibly connected) manifold of equilibrium points where the process can be stabilized, which we denote as the candidate safe-park set $X_c := \{x_c \in \mathbb{R}^n : f(x_c) + g^1(x_c)u_{failed}^1 + \sum_{i=2}^m g^i(x_c)u_2^i = 0,\ u_{min}^i \leq u_2^i \leq u_{max}^i, i = 2, \dots, m\}$. The safe-park candidates represent equilibrium points that the system can be stabilized at, subject to the failed actuator, and with the other manipulated inputs within the allowable ranges. Note that if $u_{failed}^1 \neq 0$, then it may happen that $0 \notin X_c$, i.e., if the failed actuator is frozen at a non-nominal value, then it is possible that the process simply cannot be stabilized at the nominal equilibrium point using the functioning control actuators. Maintaining the functioning actuators at the nominal values may drive the process state to a point from where it may not be possible to resume nominal operation upon fault-recovery, or even if possible, may not be 'optimal'. We define the safe-parking problem as the one of identifying safe-park points $x_s \in X_c$ that allow efficient resumption of nominal operation upon fault-recovery.

B. Safe-parking to resume nominal operation

In this section, we present a safe-parking framework and a controller that executes safe-parking as well as resumption of nominal operation. To account for the presence of constraints on the manipulated inputs, the key requirements for a safe-park point include that the process state at the time of the failure resides in the stability region for the safe-park point (so the process can be driven to the candidate safe-park point), and that the safe-park point should reside in the stability region under nominal operation (so the process can be returned to nominal operation). These requirements are formalized in Theorem 2 below. To this end, consider the system of Eq.1 for which the first control actuator fails at a time T^{fault} and is reactivated at time $T^{recovery}$, and for which the stability region under nominal operation, denoted by Ω_n, has been characterized using the predictive controller formulation of Eqs.2–6. Similarly, for a candidate safe-park point x_c, we denote Ω_c as the stability region (computed a priori) under the predictive controller of Eqs.2–6, and u_{2,x_c} as the control law designed to stabilize at the candidate safe-park with $u_{1,n}$ being the nominal control law.

Theorem 2: *Consider the constrained system of Eq.1 under the MPC law of Eqs.2–6. If $x(T^{fault}) \in \Omega_c$ and $\Omega_c \subset \Omega_n$, then the switching rule*

$$u(t) = \left\{ \begin{array}{lcl} u_{1,n} & , & 0 \leq t < T^{fault} \\ u_{2,x_c} & , & T^{fault} \leq t < T^{recovery} \\ u_{1,n} & , & T^{recovery} \leq t \end{array} \right\} \quad (9)$$

guarantees that $x(t) \in \Omega_n\ \forall\ t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d$.

Proof of Theorem 2: We consider the two possible cases; first if no fault occurs ($T^{fault} = T^{recovery} = \infty$), and second if a fault occurs at a time $T^{fault} < \infty$ and is recovered at a time $T^{fault} \leq T^{recovery} < \infty$.

Case 1: The absence of a fault implies $u(t) = u_{1,n}\ \forall\ t \geq 0$. Since $x(0) \in \Omega_n$, and the nominal control configuration is implemented for all times, we have from Theorem 1 that $x(t) \in \Omega_n\ \forall\ t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d$.

Case 2: At time T^{fault}, the control law designed to stabilize the process at x_c is activated and implemented till $T^{recovery}$. Since $x(T^{fault}) \in \Omega_c \subset \Omega_n$, we have that $x(t) \in \Omega_n\ \forall\ T^{fault} \leq t \leq T^{recovery}$. At a time $T^{recovery}$, we therefore also have that $x(T^{recovery}) \in \Omega_n$. Subsequently, as with case 1, the nominal control configuration is implemented for all time thereafter, we have that $x(t) \in \Omega_n\ \forall\ t \geq T^{recovery}$. In conclusion, we have that

$x(t) \in \Omega_n \; \forall \; t \geq 0$ and $\limsup_{t \to \infty} \|x(t)\| \leq d$. This completes the proof of Theorem 2.

Remark 2: The statement of Theorem 2 requires that for a safe-park point, the stability (and invariant) region be such that the process state at the time of the failure resides in the stability region for the safe-park point so the process can be driven to the point of safe-park with the depleted control action available. Note that this characterization can be done off-line. Specifically, for a fail-safe position of an actuator, the entire set of candidate safe-park points X_c can be computed off-line, and also, for any given point in this set, the stability region subject to depleted control action can also be computed off-line. The statement of the theorem also requires that the stability (and invariant) region for a safe-park point be completely contained in the stability region under nominal operation, so the state trajectory always stays within the stability region under nominal operation. This requirement can be readily relaxed to only require that the state at the time of the failure reside in the stability region of the safe-park point. This will allow for the state trajectory to leave the stability region, Ω_n, during the time of fault recovery. However, to preserve closed–loop stability upon fault-recovery, the control law utilizing depleted control action may be continued up until the time that the state trajectory enters the stability region under nominal operation (this is guaranteed to happen because $x_c \in \Omega_n$), after which the control law utilizing all the manipulated inputs can be implemented to achieve closed–loop stability.

Remark 3: Note that the assumption that the failed actuator reverts to the fail-safe position allows enumerating the possible fault situations for any given set of manipulated inputs a-priori to determine the safe-park candidates and then pick the appropriate safe-park point online (the condition $x_s \in \Omega_n$ can be verified off-line, however $x(T^{fault}) \in \Omega_{x_s}$ can only be verified online, upon fault-occurrence;). The assumption reflects the practice wherein actuators have a built-in fail-safe position that they revert to upon failure. Note that while the proposed safe-parking framework assumes *apriori* knowledge of the fail-safe positions of the actuators, it does not require a priori knowledge of the fault and recovery times, and only provides appropriate switching logic that is executed when and if a fault takes place and is subsequently rectified. Note also that while the statement of Theorem 2 considers faults in one of the actuators, generalizations to multiple faults (simultaneous or otherwise) are possible, albeit involving the expected increase in off-line computational cost (due to the necessity of determining the safe-park points for all combinations of the faults in the control actuators).

C. Incorporating performance considerations in safe-parking

In the previous section, the requirements for an equilibrium point to be denoted a safe-park point was provided. A large set of equilibrium points may qualify as safe-park points and satisfy the requirements in Theorem 2. In this section, we introduce performance considerations in the eventual choice of the 'optimal' safe-park point. To this end, consider again the system of Eq.1 for which the first control actuator fails at a time T^{fault} and is reactivated at time $T^{recovery}$, and for which the set of safe-park points, $x_s \in X_s$, have been characterized. For a given safe-park point (one that satisfies the requirements of Theorem 2), define the followings costs:

$$J_{tr} = \int_{T^{fault}}^{T^{fault}+T_s} \left[\|x^u(s;x,t)\|_{Q_{tr}^2} + \|u(s)\|_{R_{tr}^2} \right] ds \tag{10}$$

where Q_{tr} and R_{tr} are positive definite matrices, the subscript tr signifying that this value captures the 'cost' associated with transitioning to the safe-park point, with T_s being the time required to go to a sufficiently close neighborhood of the safe-park point. This cost can be estimated online, upon fault-occurrence, by running fast simulations of the closed–loop system under the bounded controller (for further discussion on this issue, see Remark 5). Similarly, define

$$J_s \quad = \quad f_s(x_s, u_s) \tag{11}$$

where $f_s(x_s, u_s)$ is an appropriately defined cost function and the subscript s denotes that this value captures the 'cost' associated with operating at the safe-park point. Unlike the cost in Eq.10, this cost does not involve an integration over time, and can be determined off-line. Finally, define

$$J_r \quad = \quad \int_0^{T_r} \left[\|x^u(s;x,t)\|_{Q_r^2} + \|u(s)\|_{R_r^2} \right] ds \tag{12}$$

where Q_r and R_r are positive definite matrices, with the subscript r signifying that this value captures the 'cost' associated with resuming nominal operation, with T_r being the time required to return to a sufficiently close neighborhood of the nominal operating point, and the integration performed with the safe-park point as the initial condition. Again, this cost can be estimated off-line by running simulations of the closed–loop system under the bounded controller. Consider now the safe-park points $x_{s,i} \in X_s, i = 1, \ldots, N_s$ where N_s is the number of safe-park points to be evaluated for optimality and let $J_{x_{s,i}} = J_{tr,i} + J_{s,i} + J_{r,i}$, $i = 1, \ldots, N_s$.

Theorem 3: *Consider the constrained system of Eq.1 under the MPC law of Eqs.2–6 and the switching rule*

$$u(t) = \left\{ \begin{array}{ccc} u_{1,n} & , & 0 \leq t < T^{fault} \\ u_{2,x_{s,o}} & , & T^{fault} \leq t < T^{recovery} \\ u_{1,n} & , & T^{recovery} \leq t \end{array} \right\} \tag{13}$$

where $o \in \{1, \ldots N_s\} = arg \min_{i=1,N_s} J_{x_{s,i}}$ *guarantees that* $x(t) \in \Omega_n \; \forall \; t \geq 0$ *and* $\limsup_{t \to \infty} \|x(t)\| \leq d$.

Proof of Theorem 3: Any $x_{s,o}$ chosen according to Theorem 3 satisfies the requirements of Theorem 2. $x(t) \in \Omega_n \; \forall \; t \geq 0$ and $\limsup_{t \to \infty} \|x(t)\| \leq d$ follow from the proof of Theorem 2.

Remark 4: Note that the cost of transitioning to the safe-park point J_{tr} can be estimated using the bounded controller since the bounded controller achieves decay of the same Lyapunov function as that used in the predictive controller design. This cost has to be estimated online, because it depends on the process state at which the failure occurs (in the special case that faults occur after the process has been stabilized at the nominal operating points, this cost can also be computed off-line). In contrast, the cost incurred in resuming nominal operation from the safe-park point can be computed off-line by running simulation under the predictive controller or auxiliary controller. Additional terms in J_{tr} and J_s can be readily included to cater to the specific process under consideration. Furthermore, the contribution of the cost J_s to the total cost can be appropriately scaled utilizing reasonable estimates of fault-rectification times. Specifically, if the malfunctioned actuator is known to require significant time to be rectified, then this cost can be 'weighed' more to recognize the fact that the process will deliver substantial amount of product corresponding to the safe-park point under consideration. If, on the other hand, it is known that the fault can be rectified soon, then the cost involving the resumption to nominal operation J_r can be given increased weight.

Remark 5: For the 'product' being generated during safe-parking, further unit operations may be required, ranging from simple separations to further processing, all of which may have associated costs. Possible loss of revenue during safe-park can be incorporated in the estimate J_s. If the process is connected to further units downstream, then increased utility costs associated with downstream processing can also be accounted for in this cost. Finally, we note that the costs outlined here are only some of the representative costs, and the framework allows for incorporating costs/revenues that may be specific to the process under consideration.

Remark 6: Note that while the set of safe-parking points (satisfying the requirements of Theorem 2) could be a continuous manifold of equilibrium points, safe-parking points to be evaluated for optimality can be picked by discretizing the manifold. The minimization in determining the optimal safe-park point can then be carried out by a simple procedure of comparison of the cost estimates associated with the finite number of safe-parking candidates. Choosing a finer discretization in evaluating the safe-parking candidates could possibly yield improved closed–loop costs, however, the approximations involved in the cost estimation (the cost of going to and returning from the safe-parking points are only approximately estimated using the bounded controller) could offset the benefits out of the finer discretization. Therefore, a balance has to be struck in picking the number of safe-parking points that will be evaluated for optimality that trades off the increased computational complexity, the approximations in cost estimation, and the improved performance derived out of the finer discretization.

D. Illustrative simulation example

We illustrate in this section the proposed safe-park framework via a continuous stirred tank reactor (CSTR). Consider a CSTR where an irreversible, first-order exothermic reaction of the form $A \xrightarrow{k} B$ takes place. The mathematical model for the process takes the form:

$$\dot{C_A} = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{RT_R}} C_A$$
$$\dot{T_R} = \frac{F}{V}(T_{A0} - T_R) + \frac{(-\Delta H)}{\rho c_p} k_0 e^{\frac{-E}{RT_R}} C_A + \frac{Q}{\rho c_p V} \quad (14)$$

where C_A denotes the concentration of the species A, T_R denotes the temperature of the reactor, Q is the heat added to/removed from the reactor, V is the volume of the reactor, k_0, E, ΔH are the pre-exponential constant, the activation energy, and the enthalpy of the reaction and c_p and ρ are the heat capacity and fluid density in the reactor. The values of all process parameters can be found in [17]. The control objective is to stabilize the reactor at the unstable equilibrium point $(C_A^s,\ T_R^s) = (0.447\ Kmol/m^3, 393\ K)$. Manipulated variables are the rate of heat input/removal, Q, and inlet concentration of species A, C_{A0}, with constraints: $|Q| \leq 32\ KJ/s$ and $0 \leq C_{A0} \leq 2\ Kmol/m^3$. The heat input/removal Q consists of heating stream Q_1 and cooling stream Q_2 with the constraints on each as, $0\ KJ/s \leq Q_1 \leq 32\ KJ/s$ and $-32\ KJ/s \leq Q_2 \leq 0\ KJ/s$. The nominal operating point (N) corresponds to steady state values of the inputs $C_{A0} = 0.73\ Kmol/m^3$ and $Q = 10\ KJ/s$.

For stabilizing the process at the nominal equilibrium point, the Lyapunov based MPC of Section II-B is designed using a quadratic Lyapunov function of the form $V = x^T P x$. The stability region is estimated and denoted by Ω in Fig.1. We consider the problem of designing a safe-parking framework to handle temporary faults in the heating valve (resulting in a fail-safe value of $Q_1 = 0$). In this scenario, no value of the functioning manipulated inputs $-32\ KJ/s \leq Q_2 < 0\ KJ/s$ and $0 \leq C_{A0} \leq 2\ Kmol/m^3$ exists such that the nominal equilibrium point continues to be an equilibrium point of the process subject to the fault. For $Q_2 = -14.7\ KJ/s$, $C_{A0} = 1.33\ Kmol/m^3$ and $Q_2 = -4\ KJ/s$, $C_{A0} = 1.27\ Kmol/m^3$, the corresponding equilibrium points are $S_1 = (1.05\ Kmol/m^3, 396\ K)$ and $S_2 = (0.93\ Kmol/m^3, 393\ K)$, which we denote as safe-park candidates. For each of these safe-park candidates, Lyapunov based predictive controller with prediction and control horizons of $0.10\ min$ and $0.02\ min$, respectively, is designed. The discretized version of the stability constraint of the form $V(x(t+\Delta)) \leq 0.99V(x(t))$ is incorporated in the optimization problem. If the optimization problem becomes infeasible during implementation, the stability constraint is removed to compute a solution.

Consider a scenario where the process starts from $O = (1.25\ Kmol/m^3,\ 385\ K)$ and the predictive controller drives the process toward the nominal operating point, $N =$

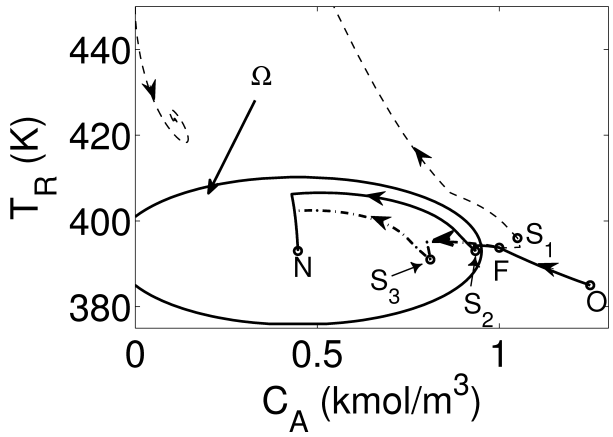

Fig. 1. Evolution of closed–loop states for the CSTR example. Dashed line (- -) indicates the case when a safe-park point S_1 is arbitrarily chosen (resulting in the inability to resume nominal operation upon fault-recovery) while the solid line (—) indicates the case when S_2 is chosen according to Theorem 2, guaranteeing resumption of nominal operation upon fault-recovery. The dash-dotted lines show the closed–loop response when optimality considerations are included in the choice of the safe-park point and S_3 is chosen.

$(0.447\ Kmol/m^3,\ 393\ K)$. At $t = 0.16\ min$, when the process state is at $F = (0.9975\ Kmol/m^3,\ 394.02\ K)$, the heating valve fails, and reverts to the fail-safe position (completely shut) resulting in $Q_1 = 0\ KJ/s$. This restricts the heat input/removal to $-32\ KJ/s \leq Q < 0\ KJ/s$ instead of $-32\ KJ/s \leq Q < 32\ KJ/s$. We first consider the case where the safe-park candidate S_1 is arbitrarily chosen as the safe-park point, and the process is stabilized at S_1 until the fault is rectified. At $t = 8.0\ min$, the fault is rectified, however, we see that even after fault-recovery, nominal operation cannot be resumed (see dashed lines in Fig.1). This happens because S_1 lies outside the stability region under nominal operation. In contrast, if S_2 is chosen as the safe-park point, we see that the process can be successfully driven to S_2 with limited control action as well as it can be successfully driven back to N after fault-recovery (see solid lines in Fig.1). In summary, the simulation scenario illustrates the necessity to account for the presence of input constraints (characterized via the stability region) in the choice of the safe-park point.

Next, we demonstrate the incorporation of performance criterion in selecting the safe-park point. To this end, we consider another point S_3 (corresponding to $Q_2 = -14.6\ KJ/s$, $C_{A0} = 1.53\ Kmol/m^3$), which is also viable safe-park point as it is inside the stability region of N. Using the approach in Section III-C, the cost associated with operating at the two safe-park points is calculated utilizing, $f(x_s, u_s) = \|x^u_{ss}\|_{Q^2_s} + \|u_{ss}\|_{R^2_s}$. At the time of the failure, the bounded controller [3], [11] is used to estimate J_{tr} and J_r, which are divided by T_s and T_r, to determine $J_{safe-parking} = \frac{J_{tr}}{Ts} + J_s + \frac{J_r}{T_r}$. Note that the computation of $J_{safe-parking}$ does not require prior information about the time of fault recovery. Also, note that here only two safe-park points are used as illustration, but the cost comparison can be carried out over larger number of safe-park points (see [17] for an application of the proposed safe-parking framework on a polystyrene process example).

The $J_{safe-parking}$ for S_2 and S_3 calculated by auxiliary controller are 2406 and 1209, respectively. The cost estimate for S_3 is significantly lower than for S_2 indicating that S_3 is a better choice for safe-parking the process. Subsequently, if S_3 is chosen as the safe-park point, it yields a closed–loop cost of 1105 which is significantly lower than the closed–loop cost for S_2 of 4072.

In summary, a safe-parking framework was developed for handling faults that preclude the possibility of continued operating at the nominal equilibrium point. Stability region is used to select the safe-park points which enables smooth resumption of the nominal operation on fault recovery. Performance considerations, such as ease of transition from and to the safe-park point and cost of running the process at the safe-park point, were then quantified and utilized in choosing the optimal safe-park point. The proposed framework was illustrated using a chemical reactor example.

REFERENCES

[1] P. D. Christofides, J. F. Davis, N. H. Farra, D. Clark, K. R. D. Harris, and J. N. G. Jr., "Smart plant operations: Vision, progress and challenges," *AIChE J., in press*, 2007.

[2] Z. D. Wang, B. Huang, and H. Unbehauen, "Robust reliable control for a class of uncertain nonlinear state-delayed systems," *Automatica*, vol. 35, pp. 955–963, 1999.

[3] Y. Lin and E. D. Sontag, "A universal formula for stabilization with bounded controls," *Syst. & Contr. Lett.*, vol. 16, pp. 393–397, 1991.

[4] S. Valluri and M. Soroush, "Analytical control of SISO nonlinear processes with input constraints," *AIChE J.*, vol. 44, pp. 116–130, 1998.

[5] N. Kapoor and P. Daoutidis, "Stabilization of nonlinear processes with input constraints," *Comp. & Chem. Eng.*, vol. 24, pp. 9–21, 2000.

[6] D. Q. Mayne, J. B. Rawlings, C. V. Rao, and P. O. M. Scokaert, "Constrained model predictive control: Stability and optimality," *Automatica*, vol. 36, pp. 789–814, 2000.

[7] S. Dubljevic and N. Kazantzis, "A new Lyapunov design approach for nonlinear systems based on Zubov's method," *Automatica*, vol. 38, pp. 1999–2005, 2002.

[8] P. Mhaskar, N. H. El-Farra, and P. D. Christofides, "Predictive control of switched nonlinear systems with scheduled mode transitions," *IEEE Trans. Automat. Contr.*, vol. 50, pp. 1670–1680, 2005.

[9] P. Mhaskar, N. H. El-Farra, and P. D. Christofides, "Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control," *Syst. & Contr. Lett.*, vol. 55, pp. 650–659, 2006.

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

[11] N. H. El-Farra and P. D. Christofides, "Bounded robust control of constrained multivariable nonlinear processes," *Chem. Eng. Sci.*, vol. 58, pp. 3025–3047, 2003.

[12] N. H. El-Farra and P. D. Christofides, "Coordinating feedback and switching for control of hybrid nonlinear processes," *AIChE J.*, vol. 49, pp. 2079–2098, 2003.

[13] P. Mhaskar, A. Gani, N. H. E.-F. C. McFall, P. D. Christofides, and J. F. Davis, "Integrated fault-detection and fault-tolerant control for process systems," *AIChE J.*, vol. 52, pp. 2129–2148, 2006.

[14] P. Mhaskar, "Robust model predictive control design for fault-tolerant control of process systems," *Ind. & Eng. Chem. Res.*, vol. 45, pp. 8565–8574, 2006.

[15] P. Mhaskar, C. McFall, A. Gani, P. D. Christofides, and J. F. Davis, "Isolation and handling of actuator faults in nonlinear systems," *Automatica* regular paper in press.

[16] P. Mhaskar, N. H. El-Farra, and P. D. Christofides, "Robust hybrid predictive control of nonlinear systems," *Automatica*, vol. 41, pp. 209–217, 2005.

[17] R. Gandhi and P. Mhaskar, "Safe-parking of nonlinear process systems," *Comp. & Chem. Eng.,* accepted for publication.