2009 American Control Conference
Hyatt Regency Riverfront, St. Louis, MO, USA
June 10-12, 2009

A Safe-parking framework for plant-wide fault-tolerant control*

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

Abstract— **This work considers the problem of plant-wide fault-tolerant control. We develop a safe-parking framework to handle actuator faults that preclude nominal unit operation. We consider the cases where the effect of the actuator fault can be contained to the faulty unit, as well as where appropriate action needs to be taken in downstream units to preserve nominal plant operation. The implementation of the safe-parking framework is illustrated using a multi-unit chemical reactor system.**

Key words: Plant-Wide Fault Tolerant Control, Safe-Parking, Nonlinear Process Systems, Actuator Faults.

I. Introduction

The operation of chemical processes often encounters faults in process equipments such as actuators and sensors. Equipment failure can have a serious impact on the product quality, can lead to undesirable pollutant emissions and can impact the overall plant productivity and economy negatively. To overcome these problems, significant research efforts have focussed on devising automated methods for online diagnosis and isolation of faults and in developing online strategies for preventing and minimizing performance degradation and smooth repair to nominal operation.

Fault tolerant control (FTC) methods can be categorized within the robust/reliable, and reconfiguration-based fault-tolerant control approaches. Robust/reliable control approaches (e.g., see [1]) essentially rely on the robustness of the active control configuration to handle faults as disturbances while reconfiguration-based fault tolerant control approaches (e.g., [2], [3], [4]) rely on existence of backup, redundant control configuration. Most of the results in fault-tolerant control (FTC) (see, e.g., [5], [2], [4], [6]) have been developed based on the assumption of availability of sufficient control effort or redundant control configurations to preserve operation at the nominal equilibrium point in the presence of faults. In contrast, the problem of faults that do not allow continuation of operation at the nominal operating point has not received sufficient attention. Specifically, the scenario where a fault results in temporary loss of stability that cannot be handled by redundant control loops has not been explicitly addressed within reconfiguration-based or reliable control approaches. In the absence of a framework to handle such faults, ad-hoc approaches could result in temporarily shutting down the process which can have negative economic ramifications.

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

†Corresponding author: mhaskar@mcmaster.ca

In [7], a safe-parking framework was developed to address the problem of determining how to run an isolated unit during fault-rectification to prevent onset of hazardous situations and enable smooth transition to nominal operation upon fault repair. In [8], the safe-parking framework is extended to handle uncertainty and limited availability of measurements. The results in [7], [8], however, consider safe-parking in the context of an isolated unit. The opportunities and challenges that arise in a plant-wide setting due to the connected nature of chemical processes via material, energy or communication lines simply do not exist in an isolated unit. The results in [7], [8] therefore cannot be applied to a plant-wide setting. Infact, a simple application of the results in [7], [8] to a multi-unit setting can result in missed opportunities as well as inadequate safe-parking. In particular, a change in operating condition of one unit naturally acts as a disturbance to the downstream units and hence large changes in operating conditions of one unit, while possibly enabling safe-parking of the unit in question, can jeopardize the operation of the downstream units, and therefore of the whole plant. This necessitates that the safe-park point for a unit in multi-unit processes be chosen with adequate consideration of its effect on downstream units.

Motivated by above considerations, this work addresses the problem of handling actuator faults in the context of multi-unit processes. We consider a multi-unit nonlinear process system subject to input constraints and faults in one unit that preclude the possibility of operating the unit at its nominal equilibrium point. We first consider in Section III-B the case where there exists a safe-park point for the faulty unit such that its effect can be completely rejected in the downstream unit. Steady-state as well as dynamic considerations (including the presence of input constraints) are used in determining the necessary conditions for safe-parking the multi-unit system. We next consider in Section III-C the problem where no viable safe-park point for the faulty unit exists such that its effect can be completely rejected in the subsequent unit. A methodology is developed that allows simultaneous safe-parking of the consecutive units. The details of the framework are illustrated using a chemical process with two chemical reactors in Section IV.

II. Preliminaries

In this section, we describe the class of processes considered and review Lyapunov-based predictive controller designs and safe-parking framework for an isolated unit.

A. Process description

Consider a plant comprising M units described by the following equations:

$$\begin{aligned} \dot{x}_1 &= f_1(x_1) + G_1(x_1)(u_1 + h_1) \\ \dot{x}_2 &= f_2(x_2) + G_2(x_2)(u_2 + h_2) + W_{2,1}(x_2)x_1 \\ &\vdots \end{aligned} \tag{1}$$

$$\dot{x}_M = f_M(x_M) + G_M(x_M)(u_M + h_M) + W_{M,M-1}(x_M)x_{M-1}$$

where $x_i := [x_i^1\ x_i^2 \cdots x_i^{n_i}]' \in \mathbb{R}^{n_i}\ i \in [1,\ M]$ denotes the vector of state variables for the i^{th} unit and $u_i(t) := [u_i^1\ u_i^2 \cdots u_i^{m_i}] \in \mathbb{R}^{m_i}$ denotes the vector of constrained manipulated variables for the i^{th} unit, taking values in a nonempty convex subset $\mathbf{U_i}$ of $\mathbb{R}^{m_i}$, where $\mathbf{U_i} = \{u_i \in \mathbb{R}^{m_i} : u_{i,min} \leq u_i \leq u_{i,max}\}$, where $u_{i,min}, u_{i,max} \in \mathbb{R}^{m_i}$ denote the constraints on the manipulated variables of the i^{th} unit. $h_i(t) := [h_i^1\ h_i^2 \cdots h_i^{m_i}] \in \mathbb{R}^{m_i}$ is a vector that captures the effect of the actuator faults on the process states. $h_i^j = 0$ for $t < t_{i,f}^j$ and $t > t_{i,r}^j$; $h_i^j = -u_i^j + u_{i,failed}^j$ for $t_{i,f}^j \geq t \geq t_{i,r}^j$, where $t_{i,f}^j$ and $t_{i,r}^j$ denote the fault occurrence and recovery times and $u_{i,failed}^j$ denotes the fail-safe value for the j^{th} actuator in the i^{th} unit. The vector function $f_i(x_i)$ and the matrix functions $G_i(x_i) = [g_i^1(x_i) \cdots g_i^{m_i}(x_i)]$ where $g_i^j(x_i) \in \mathbb{R}^{n_i}$, $j = 1 \cdots m_i$ and $W_{i,j}(x_i) = [w_{i,j}^1(x_i) \cdots w_{i,j}^{n_j}(x_i)]$ where $w_{i,j}^k(x_i) \in \mathbb{R}^{n_i}$, $k = 1 \cdots n_j$ constitute the process model for the i^{th} unit. $W_{i,j}$ captures the effect of the j^{th} unit on the i^{th} unit. It is assumed that the origin, $x_i = \mathbf{0}$, $i = 1 \cdots M$ is the nominal equilibrium point for each unit. Functions $f_i(x_i)$, $G_i(x_i)$ and $W_{i,i-1}(x_i)$, $i = 1 \cdots M$ are assumed to be sufficiently smooth on their domain of definition. The units are connected in series via material or energy streams. The results in the paper are applicable to system of the form of Eq.1, where evolution of the states in the i^{th} unit depends only on local states, local inputs and state variables of the preceding unit (through the interconnection $W_{i,i-1}(x_i)$ term). 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 $f(\cdot)$. $V(x)$ is a Lyapunov function and $L_G V = [L_{g^1} V\ \cdots\ L_{g^m} V]$, $L_W V = [L_{w^1} V\ \cdots\ L_{w^p} V]$. The notation $B \backslash A$, where A and B are sets, refers to the relative complement, defined by $B \backslash A = \{x \in B : x \notin A\}$. Throughout the manuscript, we assume that for any $u_i \in \mathbf{U_i}$ the solution of the each subsystem of Eq.1 exists and is continuous for all t, and we focus on the state feedback problem where $x_i(t),\ i = 1 \cdots M$ is assumed to be available for all t.

B. Lyapunov-based predictive controller

In this section, we review a Lyapunov-based predictive controller that handles non-linearity, uncertainty, input constraints and provides explicit characterization of stability region. We consider the k^{th} unit of the system in Eq.1 in fault-free scenario, i.e. $h_k(t) = 0$, (and drop the subscript k for simplicity) described by:

$$\dot{x} = f(x) + G(x)u + W(x)\theta \tag{2}$$

where x denotes process states of the process unit under consideration, u denotes the manipulated variables and θ is the vector of vanishing disturbances (in the sense that the nominal equilibrium point continues to be an equilibrium point in presence of disturbances; in context of multi-unit processes, θ denotes process state of upstream unit). In the predictive control formulation of [8], the control action is computed by solving an optimization problem of the form:

$$u_{MPC}(x, x_{eq}, u_{min}, u_{max}, \theta_{min}, \theta_{max}) = \arg min\{J(x,t,u(\cdot))|u(\cdot) \in S\} \tag{3}$$

$$s.t.\ \ \dot{x} = f(x) + G(x)u \tag{4}$$

$$\sup_{\theta \in \Theta} \inf_{u \in \mathbf{U}} L_f V(x) + L_W V(x)\theta + L_G V(x)u + \rho V(x) \leq 0$$

$$x(\tau) \in\ \Pi\ \forall\ \tau \in [t, t + \Delta) \tag{5}$$

$u_{MPC}(x, x_{eq}, u_{min}, u_{max}, \theta_{min}, \theta_{max})$ is Lyapunov based model predictive controller designed to stabilize the process at x_{eq} with constraints on the inputs as $u_{min} < u(t) < u_{max}$ (defined by the set U) in the presence of uncertainty that is bounded between θ_{min} and θ_{max} i.e. $\theta_{min} < \theta(t) < \theta_{max}$ (defined by the set Θ). $S = S(t, T)$ is the family of piecewise continuous functions (functions continuous from the right), with period Δ, mapping $[t, t + T]$ into U. Eq.4 is the 'nominal' nonlinear model (without the uncertainty term) describing the time evolution of the state x. A control $u(\cdot)$ in S is characterized by the sequence $\{u[j]\}$ where $u[j] := u(j\Delta)$ and satisfies $u(t) = u[j]$ for all $t \in [j\Delta, (j + 1)\Delta)$. The performance index is given by

$$J(x, t, u(\cdot)) = \int_t^{t+T} \left[\|x^u(s; x, t)\|_Q^2 + \|u(s)\|_R^2\right] ds \tag{6}$$

where Q and R are positive semi-definite, and strictly positive definite, symmetric matrices, respectively, and $x^u(s; x, t)$ denotes the solution of Eq.4, due to control u, with initial state x at time t and T is the specified horizon. The minimizing control $u_{MPC}^0(\cdot) \in S$ is then applied to the plant over the interval $[t, t + \Delta)$ and the procedure is repeated indefinitely.

To characterize the stability region for the Lyapunov-based robust MPC, a set Π is defined as,

$$\Pi = \{x \in \mathbb{R}^n : \sup_{\theta \in \Theta} \inf_{u \in \mathbf{U}} L_f V(x) + L_W V(x)\theta + L_G V(x)u + \rho V(x) \leq 0\} \tag{7}$$

An estimate of the stability region can be constructed using a level set of V, i.e

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

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

Theorem 1. [8] *Consider the constrained system of Eq.2 under the MPC law of Eqs.3–6. Then, given any positive real number ϵ, there exists a positive real number Δ^* such that if $\Delta \in (0, \Delta^*]$ and $x(0) := x_0 \in \Omega$, then the optimization problem of Eqs.3-6 is guaranteed to be initially and successively feasible, $x(t) \in \Omega \ \forall \ t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq \epsilon$. Furthermore, if $x_0 \in \Pi \backslash \Omega$, then if the optimization problem is successively feasible, then $x(t) \in \Pi \ \forall \ t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq \epsilon$.*

C. Safe-parking of an isolated unit

In this section, we briefly review the safe-parking framework for an isolated unit proposed in [7]. Assume that a fault occurs in the first actuator $u^1(t)$ of the k^{th} unit at time T^{fault} and reverts to fail-safe position u^1_{failed} with $u^1_{min} \leq u^1_{failed} \leq u^1_{max}$, and subsequently the fault is rectified at a time T^{repair}. This implies that $t^1_f = T^{fault}$ and $t^1_r = T^{repair}$. This leaves only u^i, $i = 2 \dots m$ available during $T^{fault} < t \leq T^{repair}$ for feedback control of the unit. Examples of fail-safe positions include fully open for a valve controlling a coolant flow rate and fully closed for a valve controlling a steam flow etc. In this failure scenario, there exists a set of equilibrium points where the unit can be stabilized, which we denote as the candidate safe-park set: $X_c := \{x_c \in \mathbb{R}^n : f(x_c) + g^1(x_c)u^1_{failed} + \sum_{i=2}^{m} g^i(x_c)u^i = 0, \ u^i_{min} \leq u^i \leq u^i_{max}, i = 2, \dots, m\}$. The safe-park candidates therefore represent equilibrium points that the unit can be stabilized at, subject to the failed actuator, and with the other manipulated variables within the allowable ranges. Note that if $u^1_{failed} \neq 0$, then it may happen that $0 \notin X_c$, i.e., if one of the actuators fails and reverts to a fail-safe position with non-nominal value, it may happen that no admissible combination of the functioning manipulated variables exists for which the nominal equilibrium point continues to be an equilibrium point. If the controller attempts to use the functioning actuators to preserve nominal operation, it will not succeed since there does not exist an allowable value of the functioning inputs for which the nominal equilibrium point is still an equilibrium point. The states, in such an event, could possibly stabilize at an equilibrium point outside the stability region of the nominal equilibrium, thus making it impossible to resume nominal operation upon fault rectification. Even if it may be possible to resume nominal operation, it might not be the optimal way of resuming nominal operation. Thus choice of the temporary operating point is crucial for safety and performance of process operation. In [7], the safe-parking problem is defined as the one of identifying safe-park points $x_s \in X_c$ that allow efficient resumption of nominal operation upon fault-repair.

The safe-parking framework of [7] imposes the following criteria on the safe-park point: 1) the unit state at the time of failure resides in the stability region of the safe-park candidate (subject to depleted control action), so the process can be driven to the candidate safe-park point and 2) the safe-park candidate resides within the stability region of the nominal control configuration so the unit can be returned to nominal operation after fault repair. These requirements are formalized in Theorem 2 below. To this end, consider the unit of Eq.2 for which the first control actuator fails at a time T^{fault} and is reactivated at time T^{repair}, and for which the stability region under nominal operation, denoted by Ω_n, has been characterized for the robust model predictive controller of Eqs.3–6. Similarly, for a candidate safe-park point x_c, we denote Ω_c as the stability region (computed a priori) and $u_n = u_{MPC}(x, x_n, u^{x_n}_{min}, u^{x_n}_{max}, \theta_{min}, \theta_{max})$ and $u_{x_c} = u_{MPC}(x, x_c, u^{x_c}_{min}, u^{x_c}_{max}, \theta_{min}, \theta_{max})$, where $u^{x_n}_{min}$, $u^{x_n}_{max}$ and $u^{x_c}_{min}$, $u^{x_c}_{max}$ denote the constraints on the manipulated variables for stabilizing the process at the nominal and safe-parking point respectively.

Theorem 2. [7] *Consider the constrained system of Eq.2 under the robust model predictive controller of Eqs.3–6 designed to achieve (using Theorem 1) $\limsup_{t\to\infty} \|x(t)\| \leq \epsilon$ where ϵ is a given positive real number. If $x(0) \in \Omega_n$, $x(T^{fault}) \in \Omega_c$ and $\Omega_c \subset \Omega_n$, then the switching rule*

$$u(t) \quad = \quad \left\{ \begin{array}{lcl} u_n & , & 0 \leq t < T^{fault} \\ u_{x_c} & , & T^{fault} \leq t < T^{repair} \\ u_n & , & T^{repair} \leq t \end{array} \right\} \qquad (9)$$

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

Note that in a plant-wide setting, a change in operation of a unit naturally enters as a 'disturbance' in the downstream unit. Preparatory to the presentation of our results on a safe-parking framework for plant-wide fault-tolerant control, we characterize the maximum disturbance caused by safe-parking of unit k in Proposition 1 below.

Proposition 1. Consider operation of the k^{th} unit under the safe-parking framework of Theorem 2. If $x(0) \in \Omega_n$, then $\exists \ \alpha^i, \ i = 1 \cdots n_k$ such that $|x^i(t)| \leq \alpha^i, \ i = 1 \cdots n_k, \ \forall t \geq 0$

III. SAFE-PARKING OF MULTI-UNIT PROCESSES

In multi-unit processes, due to fault in one unit, if that unit is safe-parked using the framework presented in Section II-C, without considering its interaction with the other units in the plant, then it may happen that even though the faulty unit is safely operated at safe-park point, the change in operation of the faulty unit may cause a significantly large disturbance that can not be rejected in the downstream units or may even result in instability. This necessitates that the safe-park point for the faulty unit be chosen with proper consideration to its effect on downstream processes. In other words, a safe-park point should be chosen such that it has minimal adverse effect on the ability of downstream unit to continue nominal operation. In this section, we present a framework to account for the interaction of faulty units with downstream operation while choosing a safe-park point for the faulty unit.

A. Problem definition

We consider the scenario where one of the control actuators in unit k ($k \in [1\ M]$) fails and reverts to the fail-safe value. Specifically, we consider a fault occurring, without loss of generality, in the first control actuator of the k^{th} unit at a time T^{fault}, subsequently rectified at a time T^{repair} i.e. $t^1_{k,f} = T^{fault}$ and $t^1_{k,r} = T^{repair}$. This leaves only u^j_k, $j = 2 \dots m_k$ available for feedback control of the k^{th} unit. As explained in Section II-C, if $u^1_{k,failed} \neq 0$, then the origin (the nominal operating point of k^{th} unit) may no longer be an equilibrium point and hence, the k^{th} unit can no longer be operated at the nominal equilibrium point necessitating safe-parking of the k^{th} unit.

The change in operating condition of the faulty unit due to safe-parking, however, enters the downstream unit as a disturbance. We first consider the case when this disturbance is 'small enough', i.e., it can be rejected in the $k+1^{th}$ unit (i.e., in spite of change in inlet condition of $k+1^{th}$ unit, the $k+1^{th}$ unit can be maintained at nominal operation by changing the nominal values of the manipulated variables), and the rest of the plant can, therefore, be operated nominally. We next consider the possibility that, if the disturbance caused by safe-parking of k^{th} unit is very large then it may not be rejected in the $k+1^{th}$ unit, then the downstream $k+1^{th}$ unit cannot continue operation at the nominal operating point. In other words, operation of the faulty unit at the safe-park point does not allow nominal operation of the downstream unit. This then necessitates safe-parking of the $k+1^{th}$ unit to avoid any undesirable incident requiring the simultaneous safe-parking of two units.

B. Safe-parking of a single unit in a multi-unit process

Consider the fault scenario described in Section III-A where the k^{th} unit needs to be safe-parked. In the multi-unit setup, an additional criterion needs to be added to the choice of safe-park point which is that if possible, it should allow continued nominal operation in the downstream units. In this section, we provide a systematic procedure to choose safe-park point that allows continued nominal operation in the downstream units. Preparatory to the presentation of the results, we define the set:

$$D_k = \{x_k \in \mathbb{R}^{n_k} : f_{k+1}(x_{k+1,ss}) + G_{k+1}(x_{k+1,ss})u_{k+1} + W_{k+1,k}(x_{k+1,ss})x_k = 0, u_{k+1} \in U_{k+1} \in \mathbb{R}^{m_{k+1}}\} \quad (10)$$

where $x_{k+1,ss}$ is the nominal operating points in the $k+1^{th}$ unit. Therefore, D_k is the set of values of process variables (x_k) in the k^{th} unit such that if the k^{th} unit is stabilized at x_k, nominal operation in the $k+1^{th}$ unit can be maintained using allowable, although possibly different from nominal, values of the manipulated variables in the $k+1^{th}$ unit. In other words, the non-vanishing disturbance caused by change in operation of the k^{th} unit can be rejected in the $k+1^{th}$ unit at steady state via using non-nominal values of the manipulated variables. Note that $h_{k+1} = 0$ is used for calculation of the set D_k because there is no fault in the $k+1^{th}$ unit. We denote $u_{k+1,n} = u_{MPC}(x_{k+1}, x^{ss}_{k+1,n}, u^{x_n}_{k+1,min}, u^{x_n}_{k+1,max}, \theta_{k+1,min}, \theta_{k+1,max})$ as the controller designed to control the $k+1^{th}$ unit at the nominal operating point with nominal values of manipulated variables. As mentioned earlier, when the k^{th} unit is safe-parked, the controller in $k+1^{th}$ unit can maintain the nominal operation in the unit using non-nominal values of the manipulated variables. We denote this controller as $u'_{k+1,n} = u_{MPC}(x_{k+1}, x^{ss}_{k+1,n}, u'_{k+1,min}, u'_{k+1,max}, \theta_{k+1,min}, \theta_{k+1,max})$ where $u'_{k+1,min}$ and $u'_{k+1,max}$ are modified constraints on manipulated variables. Both $u_{k+1,n}$ and $u'_{k+1,n}$ are designed to stabilize the $k+1^{th}$ unit at the nominal equilibrium point but as the nominal values of the manipulated variables (and therefore of the constraints) are different for these controllers, they may have different stability regions which we denote by $\Omega_{k+1,n}$ and $\Omega'_{k+1,n}$ respectively. As before, we denote $\Omega_{k,n}$ and $\Omega_{k,c}$ as the stability region for nominal equilibrium point and the safe-park point for the k^{th} unit respectively. For a choice of safe-park point of the k^{th} unit, the maximum disturbance caused to the $k+1^{th}$ unit is denoted by $d_{k,max}$ (characterized using Proposition 1). Theorem 3 below provides the key requirements for choice of the safe-park point for the faulty unit so that the downstream units can continue nominal operation (see [9] for a proof).

Theorem 3. *Consider the constrained system of Eq.1 subject to failure in the first control actuator of the k^{th} unit at a time T^{fault}, subsequently rectified at a time T^{repair}. If $x_k(0) \in \Omega_{k,n}$ and $x_{k+1}(0) \in \Omega_{k+1,n}$, $x_{k,sf}$ is the safe-park point for the k^{th} unit satisfying $x_k(T^{fault}) \in \Omega_{k,c}$, $x_{k,sf} \in D_k$ and $\Omega_{k,c} \subset \Omega_{k,n}$ and if $x_{k+1}(T^{fault}) \in \Omega'_{k+1,n}$ then the switching rule*

$$\begin{aligned} u_k(t) &= u_{k,n}, \quad u_{k+1}(t) = u_{k+1,n} \quad 0 \leq t < T^{fault} \\ u_k(t) &= u_{k,x_c}, \quad u_{k+1}(t) = u'_{k+1,n} \quad T^{fault} \leq t < T^{repair} \\ u_k(t) &= u_{k,n}, \quad u_{k+1}(t) = u_{k+1,n} \quad T^{repair} \leq t \end{aligned}$$

under the robust model predictive controller of Eqs.3-6 with $\theta_{k+1,min} = -d_{k,max}$ and $\theta_{k+1,max} = d_{k,max}$, guarantees that $x_k(t) \in \Omega_{k,n}$, $x_{k+1}(t) \in \Omega_{k+1,n}$ for $\forall t \geq 0$ and $\limsup_{t\to\infty} \|x_k(t)\| \leq \epsilon_k$ and $\limsup_{t\to\infty} \|x_{k+1}(t)\| \leq \epsilon_{k+1}$ where ϵ_k and ϵ_{k+1} are given positive real numbers.

C. Simultaneous safe-parking of multiple units

In the last section, we presented the framework to select a safe-park point so that nominal operation in downstream units can be continued. However, it may happen that in case of fault, none of the candidate safe-park points satisfy the requirements presented in Theorem 3, i.e. $\Omega_{k,n} \cap D_k \cap X_{k,c} = 0$. In other words, there exist no safe-park point such that nominal operation of the downstream unit can be continued. This necessitates that the downstream unit also be safe-parked. However, due to the interconnected nature of the process, the procedure for safe-parking of isolated units cannot be duplicated to safe-park multiple units, and one needs a framework to simultaneously safe-park multiple units to continue the safe-operation of the entire plant. In

this section, we provide details of framework to carry out simultaneous safe-parking.

Consider the plant of Eq.1 with $\Omega_{k,n} \cap D_k \cap X_{k,c} = 0$. We recall the control laws $u_{k,n}$, u_{k,x_c} and $u_{k+1,n}$ as defined in Section III-B. Further, we define, $u_{k+1,x_c} = u_{MPC}(x_{k+1}, x^{ss}_{k+1,c}, u^{x_{k+1,c}}_{k+1,min}, u^{x_{k+1,x_c}}_{k+1,max}, \theta_{k+1,min}, \theta_{k+1,max})$ as control law to stabilize the $k+1^{th}$ unit at a candidate safe-park point $x^{ss}_{k+1,c}$. Also, we define $\Omega_{k+1,n}$ and $\Omega_{k+1,c}$ as the stability regions for the nominal equilibrium point and safe-park point in the downstream unit, for the robust predictive controller of Eqs.3–5 designed using $\theta_{k+1,min} = -d_{k,max}$ and $\theta_{k+1,max} = d_{k,max}$ where $d_{k,min}$ and $d_{k,max}$ are maximum possible disturbance that can be caused by safe-parking of k^{th} unit (characterized using Proposition 1). The key idea in simultaneous safe-parking is to ensure that for a choice of safe-park point of the faulty processing unit, there exists a safe-park point for the downstream unit (for which the 'disturbance' caused by the safe-parking of the faulty unit can be rejected) and such that it can resume nominal operation when the faulty processing unit reverts to nominal operation. This requirement is formalized in Theorem 4 (see [9] for a proof).

Theorem 4. *Consider the constrained system of Eq.1 subject to failure in the first control actuator of the k^{th} unit at a time T^{fault}, subsequently rectified at a time T^{repair}, and $x_{k,sf}$ and $x_{k+1,sf}$ are chosen as safe-park points for the k^{th} and $k+1^{th}$ unit, respectively, such that $x_k(T^{fault}) \in \Omega_{k,c}$, $x_{k+1}(T^{fault}) \in \Omega_{k+1,c}$, $\Omega_{k,c} \subset \Omega_{k,n}$ and $\Omega_{k+1,c} \subset \Omega_{k+1,n}$, then the switching rule*

$$\begin{aligned} u_k(t) &= u_{k,n}, \quad u_{k+1}(t) = u_{k+1,n} \quad 0 \le t < T^{fault} \\ u_k(t) &= u_{k,x_c}, \quad u_{k+1}(t) = u_{k+1,x_c} \quad T^{fault} \le t < T^{repair} \\ u_k(t) &= u_{k,n}, \quad u_{k+1}(t) = u_{k+1,n} \quad T^{repair} \le t \end{aligned}$$

under the robust model predictive controller of Eqs.3-6, guarantees that $x_k(t) \in \Omega_{k,n}$ and $x_{k+1}(t) \in \Omega_{k+1,n}$ for $\forall t \ge 0$, $\limsup_{t\to\infty} \|x_k(t)\| \le \epsilon_k$ and $\limsup_{t\to\infty} \|x_{k+1}(t)\| \le \epsilon_{k+1}$.

IV. Application to a two-unit chemical process

Consider a process composed of two well-mixed, non-isothermal continuous stirred-tank reactors (CSTRs) with interconnections, where three parallel irreversible elementary exothermic reactions of the form $A \xrightarrow{k_1} B$, $A \xrightarrow{k_2} U$ and $A \xrightarrow{k_3} R$ take place, where A is the reactant species, B the desired product, and U and R are the undesired byproducts. The feed to CSTR-1 consists of pure A at flow rate F_0, molar concentration C_{A0}, and temperature T_0, and the feed to CSTR-2 consists of the output of CSTR-1, and an additional fresh stream feeding pure A at flow rate F_3, molar concentration C_{A03}, and temperature T_{03}. Under standard modeling assumptions, a mathematical model of the plant can be derived and takes the following form:

$$\frac{dT_1}{dt} = \frac{F_0}{V_1}(T_0 - T_1) + \sum_{i=1}^{3} \frac{\Delta H_i}{\rho c_p} R_i(C_{A1}, T_1) + \frac{Q_1}{\rho c_p V_1}$$

$$\frac{dC_{A1}}{dt} = \frac{F_0}{V_1}(C_{A0} - C_{A1}) - \sum_{i=1}^{3} R_i(C_{A1}, T_1)$$

$$\frac{dT_2}{dt} = \frac{F_1}{V_2}(T_1 - T_2) + \frac{F_3}{V_2}(T_{03} - T_2) + \sum_{i=1}^{3} \frac{\Delta H_i}{\rho c_p} R_i(C_{A2}, T_2) + \frac{Q_2}{\rho c_p V_2}$$

$$\frac{dC_{A2}}{dt} = \frac{F_1}{V_2}(C_{A1} - C_{A2}) + \frac{F_3}{V_2}(C_{A03} - C_{A2}) - \sum_{i=1}^{3} R_i(C_{A2}, T_2)$$

where $R_i(C_{Aj}, T_j) = k_{i0} exp(E_i/RT_j) C_{Aj}$, for $j = 1, 2$. The symbols T, C_A, Q, and V denote the temperature of the reactor, the concentration of species A, the rate of heat input/removal from the reactor, and the volume of reactor, respectively, with subscript 1 denoting CSTR 1, and subscript 2 denoting CSTR 2. ΔH_i, k_i, E_i, $i = 1, 2, 3$, denote the enthalpies, pre-exponential constants and activation energies of the three reactions, respectively, c_p and ρ denote the heat capacity and density of fluid in the reactor. Q_1 and Q_2 are net heat added/removed from CSTR-1 and CSTR-2, respectively. The Q_1 term consists of heat removed $Q_{1,c}$ and heat added $Q_{1,h1}$ and $Q_{1,h2}$ (i.e. $Q_1 = Q_{1,c} + Q_{1,h1} + Q_{1,h2}$) in CSTR-1 while Q_2 consists of heat removed $Q_{2,c}$ and heat added $Q_{2,h1}$ and $Q_{2,h2}$ (i.e. $Q_2 = Q_{2,c} + Q_{2,h1} + Q_{2,h2}$) in CSTR-2. The values for all the parameters is given in [9].

The control objective is to stabilize CSTR-1 at the unstable equilibrium point ($C_{A1} = 1.69\ kmol/m^3$, $T_1 = 424.4\ K$) and CSTR-2 at the unstable equilibrium point ($C_{A2} = 0.89\ kmol/m^3$, $T_2 = 444.5\ K$). The manipulated variables for the CSTR-1 are C_{A0} and (Q_1 while manipulated variables for the CSTR-2 are C_{A30}) and Q_2. For constraints on the manipulated inputs, and details of the controller design, see [9].

To this end, consider a fault where one of the heating coils in CSTR-1 fails to its fail-safe position (resulting in $Q_{1,h2} = 0$) at time $t = 1\ hr$ and so the constraints on net heat added/removed from CSTR-1 becomes $-2 \times 10^6 \le Q_1 \le 0.5 \times 10^6\ KJ/hr$. This makes it impossible to operate CSTR-1 at the nominal equilibrium point because there exist no admissible inputs which can maintain CSTR-1 at the nominal equilibrium point and, therefore, CSTR-1 needs to be safe-parked at a safe-park point. We first consider

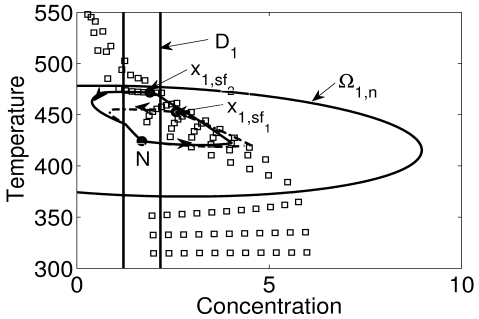

Fig. 1. Stability region for nominal equilibrium point ($\Omega_{1,n}$), the set D_1 and candidate safe-park points (□) for fail-safe value of $Q_{1,h1}$ for CSTR-1. Dashed lines (- -) indicate the case when x_{1,sf_1} is chosen as the safe-park point for CSTR-1 while the solid lines (—) show the case when x_{1,sf_2} is chosen as the safe-park point for CSTR-1.

the case where a fault occurs in CSTR-1 and it is safe-parked utilizing the safe-parking framework for isolated

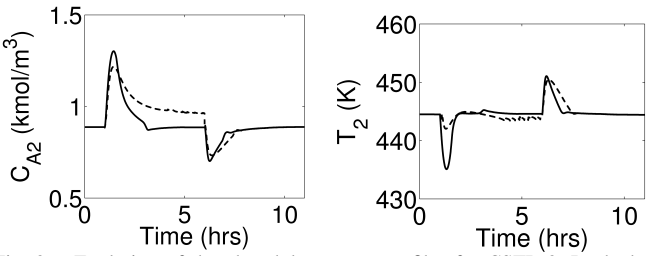

Fig. 2. Evolution of the closed–loop state profiles for CSTR-2. Dashed lines (- -) indicate the case when x_{1,sf_1} is chosen as the safe-park point for CSTR-1 while the solid lines (—) show the case when x_{1,sf_2} is chosen as the safe-park point for CSTR-1.

unit described in Section II-C. Therefore a safe-park point $x_{1,sf_1} : (C_{A1} = 2.58\ kmol/m^3,\ T_1 = 452.6\ K$ is chosen. Note that $x_{1,sf_1} \in \Omega_{k,n}$ and $N \in \Omega_{k,x_{1,sf_1}}$. It is therefore possible to stabilize CSTR-1 at the safe-park point x_{1,sf_1}. However, as can be seen from the dashed line in Fig.2, safe-parking CSTR-1 at x_{1,sf_1} does not permit operating CSTR-2 at the nominal equilibrium point. To explain this, we superimpose set D on the candidate safe-park points in Fig.1 and it can be seen that the safe-park point x_{1,sf_1} is outside the set D. This explains the inability of operating CSTR-2 at the nominal equilibrium point. In contrast, if the proposed safe-parking framework outlined in Theorem 3 is utilized, it dictates picking $x_{1,sf_2} : (C_{A1} = 1.90\ kmol/m^3,\ T_1 = 471.6\ K)$ as the safe-park point, since x_{1,sf_2} is inside the stability region of nominal equilibrium point and inside the set D (i.e $x_{1,sf_2} \in \Omega \cap D$) as well. Choice of x_{1,sf_2} ensures that nominal operation in CSTR-1 can be resumed upon fault repair, as demonstrated by the solid line in Fig.2. Next,

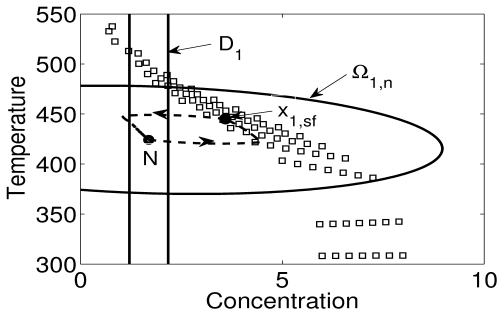

Fig. 3. Stability region for nominal equilibrium point ($\Omega_{1,n}$), the set D_1 and candidate safe-park points (□) for failure value of C_{A0} for CSTR-1. Dashed lines (- -) shows the closed loop state profiles of CSTR-1 for simultaneous safe-parking.

consider a case where a fault occurs in upstream of CSTR-1 restricting the concentration of inlet stream to $6 \leq C_{A0} \leq 8\ Kmol/m^3$ instead of $0 \leq C_{A0} \leq 8\ Kmol/m^3$. This fault makes it impossible to continue nominal operation in CSTR-1 because nominal equilibrium point is not an equilibrium point in the faulty scenario. For the simulations we design the robust predictive controller for CSTR-2 using $\theta_{max} = (0.2\ kmol/m^3,\ 20\ K)$. The stability region for nominal operating point and the set D_k as well as the set of equilibrium points in faulty scenario are shown in Fig.3. From Fig.3, it can be seen that there exist no candidate safe-park point such that $x_{1,sf} \in \Omega \cap D_k$ and hence, there exists no safe-park point for CSTR-1 such that nominal operation in CSTR-2 can be continued. This requires that both CSTR-1 and CSTR-2 be safe-parked simultaneously. Out of the safe-park candidates, we choose $x_{1,sf} : (C_{A1} = 3.59\ kmol/m^3,\ T_1 = 445.0\ K)$ as the safe-park point for CSTR-1, and $x_{2,sf} : (C_{A2} = 1.30\ kmol/m^3,\ T_2 = 437.3\ K)$ as safe-park point for CSTR-2. As can be seen from the solid lines in Fig.3 for CSTR-1 (the corresponding state profiles for CSTR-2 are shown as solid lines in Fig.4) safe-parking of both CSTR's and subsequent resumption of nominal operation (at time $t = 9\ hrs$) is achieved.

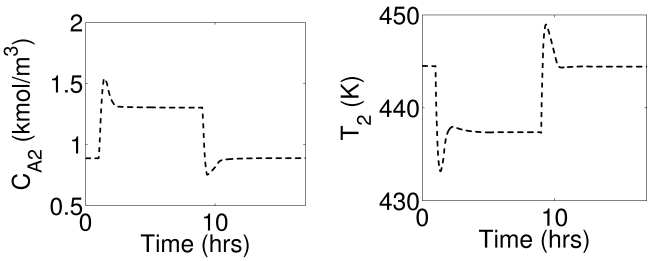

Fig. 4. Evolution of the closed–loop state profiles for CSTR-2. Simultaneous safe-parking of both CSTR's and subsequent resumption of nominal operation is successfully achieved.

In summary, a safe-parking framework for plant-wide fault-tolerant control was developed to handle faults that preclude the possibility of continued operating at the nominal equilibrium point. First a framework was developed to select the safe-park point in faulty unit such that nominal operation in downstream unit can be continued during fault rectification. Next we considered the scenario where no viable safe-park point for the faulty unit exists such that its effect can be completely rejected in the subsequent unit. A methodology was developed that allows simultaneous safe-parking of the consecutive units. The efficacy of the proposed framework was illustrated using a process comprising two chemical reactors in series.

REFERENCES

[1] 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.

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

[3] 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.

[4] P. Mhaskar, C. McFall, A. Gani, P. D. Christofides, and J. F. Davis, "Isolation and handling of actuator faults in nonlinear systems," *Automatica*, vol. 44, pp. 53–62, 2008.

[5] N. H. El-Farra, "Integrated fault detection and fault-tolerant control architectures for distributed processes," *Ind. & Eng. Chem. Res.*, vol. 45, pp. 8338–8351, 2006.

[6] A. Armaou and M. Demetriou, "Robust detection and accommodation of incipient component and actuator faults in nonlinear distributed processes," *AIChE J.* in press, vol. 54, p. 26512662, 2008.

[7] R. Gandhi and P. Mhaskar, "Safe-parking of nonlinear process systems," *Comp. & Chem. Eng.*, vol. 32, pp. 2113–2122, 2008.

[8] M. Mahmood, R. Gandhi, and P. Mhaskar, "Safe-parking of nonlinear process systems: Handling uncertainty and unavailability of measurements," *Chemical Engineering Science*, vol. 63, no. 22, pp. 5434 – 5446, 2008.

[9] R. Gandhi and P. Mhaskar, "Safe-parking framework for plant-wide fault tolerant control," *Chem. Eng. Sci.,* submitted.