NONLINEAR MPC DESIGN & APPLICATIONS

NONLINEAR MODEL PREDICTIVE CONTROL DESIGN AND APPLICATIONS

by

Maaz Mahmood, B.Eng. (Chemical), B.Sc. (Mathematical Science)

A Thesis
Submitted to the School of Graduate Studies
in Partial Fulfillment of the Requirements
for the Degree
Master of Applied Science

McMaster University

MASTER OF APPLIED SCIENCE (2009) McMaster University

(Chemical Engineering) Hamilton, Ontario, Canada

TITLE:	Nonlinear Model Predictive Control Design and Applications
AUTHOR:	Maaz Mahmood, B.Eng. (Chemical), B.Sc. (Mathematical Science)
	(McMaster University, Hamilton, Ontario, Canada)
SUPERVISOR:	Dr. Prashant Mhaskar
NUMBER OF PAGES:	xiv, 121

ABSTRACT

This thesis considers the problem of nonlinear predictive control design and applications. A predictive control formulation is presented which expands on the set of initial conditions for which closed-loop stability can be achieved. The key idea in this control design is to utilize control-law independent characterization of the process dynamics subject to constraints via model predicative controllers. An application of this idea is presented to the case of linear process systems for which characterizations of the null controllable region (the set of initial conditions from where closed-loop stability can be achieved subject to input constraints) are available. A predictive controller is designed that achieves closed-loop stability for every initial condition in the null controllable region. For nonlinear process systems, the constraints within the predictive controller are formulated to require the process to evolve within the region from where continued decay of the Lyapunov function value is achievable and incorporated in the predictive control design, thereby expanding on the set of initial conditions from where closed-loop stability can be achieved. The proposed method is illustrated using a chemical reactor example, and the robustness with respect to parametric uncertainty and disturbances demonstrated via application to a styrene polymerization process.

In addition, we also consider the application of the predictive control design to the problem of handling actuator faults in nonlinear continuous-time processes and transport-reaction systems. Specifically, we consider faults that preclude the possibility of continued operating at the nominal equilibrium point using the existing robust or reconfiguration-based fault-tolerant control approaches. The key consideration is to operate the plant using the depleted control action at an appropriate safe-park point to prevent onset of hazardous situations as well as enable smooth resumption of nominal operation upon fault-repair. For the case of continuous-time nonlinear process systems we consider the presence of input constraints, uncertainty, and availability of limited measurements. First a Lyapunov-based predictive controller with an explicitly characterized stability region is developed to handle the aforementioned conditions. This control design is then subsequently used to develop a safe-parking framework in the presence of uncertainty, and availability of limited measurements. The proposed framework is illustrated using a chemical reactor example and

demonstrated on a styrene polymerization process. Finally, we consider the problem of model predictive control and handling actuator faults in transport-reaction processes described by quasi-linear parabolic partial differential equations (PDEs) subject to input constraints. A Lyapunov-based model predictive controller is designed which accounts for the distributed nature of transport-reaction processes and provides an explicit characterization of the set of initial conditions from where closed–loop stability of the parabolic PDE system is guaranteed. Similar to the continuous time case, this control design is then subsequently used to develop a safe-parking framework for handling actuator faults in transport-reaction processes. The proposed framework is illustrated on a diffusion-reaction process

ACKNOWLEDGEMENTS

I wish to express my gratitude to my supervisor Professor Prashant Mhaskar for his guidance and support throughout my research. Also, for all the opportunities he has given me.

I would also like to thank my family. My academic success would have not been possible without the unqualified love and support from them: Mom, Dad, Sheraz, and Fraz. In addition, I would like to thank the following friends and members of my extended family for their love and encouragement: Kashif, Faraan, Maliha, Mohamad, Shakeel, and Zohaib.

I also give many thanks to the following professors for the guidance and expertise they have provided me during my undergraduate and graduate studies: Chris Swartz, Tom Marlin, Stan Alama, Miroslav Lovric, and Bartosz Protas.

Finally, I thank my beloved Hila for supporting me in the rough times and celebrating with me in joyful times; her love has seen the task completed.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

The presence of input constraints are ubiquitous in the control and operation of all physical systems. These constraints usually arise due to the physical limitation of control actuators such as pumps or valves. Neglecting to take such constraints into consideration while designing controllers can lead to significant performance deterioration and even closed–loop instability. This has motivated considerable research effort towards the problem of designing controllers in the presence of input constraints (see e.g. [54] and references therein).

One product resulting from this research effort for lumped-parameter nonlinear process systems modelled ordinary differential equations (ODEs) is that of Lyapunov-based control designs. Such designs explicitly account for the presence of constraints and are able to provide explicit characterization from where closed–loop stability can be achieved. Furthermore, Lyapunov-based controllers have also been developed within a predictive control framework. Such predictive control designs provide guaranteed stability regions alongside the incorporation of performance considerations.

Many essential industrial chemical processes involve the presence of convection and diffusion phenomena coupled with a chemical reaction. We refer to such processes as transport-reaction processes. Examples of transport-reaction processes include tubular reactors and packed-bed reactors. The dynamic models of transport-reaction processes over finite spatial

domains typically consists of highly dissipative partial differential equations (PDE). In some cases, the dissipative nature of the differential operator can be exploited to derive finite-dimensional approximate models of the infinite-dimensional system. This model reduction allows for the extension of finite-dimensional control designs (e.g. Lyapunov-based designs) to handle control problems of transport-reaction processes.

Along with actuator constraints, the control of chemical processes involves accounting for eventualities such as faults. Since faults can potentially lead to hazardous plant situations and also significant economic damage, there has been extensive research on the development of strategies for handling faults. The traditional control approaches for handling faults assume availability of sufficient residual control effort or redundant control configurations to preserve operation at the nominal equilibrium point. This approach can be categorized within the robust/reliable, and reconfiguration-based fault-tolerant control approaches. The problem of handling faults which inhibit continued operation at the nominal operating point using robust/reliable, and reconfiguration-based schemes was recently considered in [36]. Specifically, a fault-tolerant scheme was presented which temporarily maintains the process at 'safe-parking' points during fault rectification, and smoothly resumes nominal operation upon fault repair. This safe-parking framework utilizes the stability region characterizations provided by Lyapunov-based predictive control designs to identify safe-parking locations in which the onset of hazardous conditions is prevented and smooth resumption can be guaranteed.

This thesis considers the following two general problems: 1) The design of predictive controllers for nonlinear process systems and transport-reaction systems. 2) The application of the designed predictive controllers to handling faults which cannot be handled by robust/reliable, and reconfiguration-based approaches in nonlinear process systems and transport-reaction systems. The broad objectives of this thesis are as follows:

- To develop a Lyapunov-based predictive control design for continuous-time nonlinear process systems which enhances the set of initial conditions from which stability can be guaranteed by better utilizing the constraint handling capabilities of model predictive

control.

- To develop a Lyapunov-based predictive control design which maximizes the guaranteed stability region estimate for linear systems.
- To develop a Lyapunov-based predictive control design for nonlinear process systems which explicitly accounts for the presence of uncertainty and availability of limited measurements.
- To develop a Lyapunov-based predictive control design for transport-reaction process systems which provides an explicit characterization of the set initial conditions of the infinite-dimensional system from where stability is guaranteed.
- To develop a fault-tolerant safe-parking framework for nonlinear process systems which accounts for the presence of uncertainty and availability of limited measurements.
- To develop a fault-tolerant safe-parking framework for transport-reaction process systems.

The rest of this thesis is organized as follows. In chapter 2, Lyapunov-based tools are used to develop control-law independent characterizations of the stability region and this characterization is exploited via the constraints handling capabilities of model predicative controllers to expand on the set of initial conditions for which closed–loop stability can be achieved. To clearly illustrate the main idea behind the approach, we first consider linear process systems for which characterizations of the null controllable region (the set of initial conditions from where closed–loop stability can be achieved subject to input constraints) are available. A predictive controller is designed that achieves closed–loop stability for every initial condition in the null controllable region. For nonlinear process systems, while characterizing the null controllable region remains intractable, the set of initial conditions for which a (given) Lyapunov function can be made to decay can be analytically computed. Constraints are formulated requiring the process to evolve within the region from where continued decay of the Lyapunov function value is achievable and incorporated in the predictive control

design, thereby expanding on the set of initial conditions from where closed–loop stability can be achieved. The proposed method is illustrated using a chemical reactor example and the robustness with respect to parametric uncertainty and disturbances demonstrated via application to a styrene polymerization process. The author wishes to point out that the work in chapter 2 was completed prior to start of the masters program. However, a brief version of this work is retained in this thesis for completeness.

In chapter 3, the problem of handling actuator faults in nonlinear process systems subject to input constraints, uncertainty and availability of limited measurements is considered. A framework is developed to handle faults that preclude the possibility of continued operating at the nominal equilibrium point using the existing robust or reconfiguration-based fault-tolerant control approaches. The key consideration is to operate the plant using the depleted control action at an appropriate 'safe-park' point to prevent onset of hazardous situations as well as enable smooth resumption of nominal operation upon fault-repair. First, we consider the presence of constraints and uncertainty and develop a robust Lyapunov-based model predictive controller that enhances the set of initial conditions from which closed–loop stability is achieved. The stability region characterization provided by the robust predictive controller is subsequently utilized in a safe-parking algorithm that appropriately selects 'safe-park' points from the safe-park candidates (equilibrium points subject to failed actuators) to preserve closed–loop stability upon fault repair. 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 uncertainty), and 2) the safe-park candidate resides within the stability region of the nominal control configuration. Then we consider the problem of availability of limited measurements. An output feedback Lyapunov-based model predictive controller, utilizing an appropriately designed state observer (to estimate the unmeasured states), is formulated and its stability region explicitly characterized. An algorithm is then presented that accounts for the estimation errors in the implementation of the safe-parking framework. The proposed framework is illustrated using a chemical reactor example and demonstrated on a styrene polymerization process.

In chapter 4, the problem of handling actuator faults in transport-reaction processes described by quasi-linear parabolic partial differential equations (PDEs) subject to input constraints is considered. First, by exploiting the separation between the fast and slow eigenmodes of the parabolic spatial differential operator in combination with Galerkins method, a finite set of ordinary differential equations (ODE) that captures the dominant dynamics of the PDE system are constructed. This finite ODE system is used to develop a Lyapunov-based model predictive controller which provides an explicit characterization of the set of initial conditions from where closed–loop stability of the parabolic PDE system is guaranteed. This control design is then subsequently used to develop a safe-parking framework for handling faults. In particular, faults which preclude the possibility of maintaining operation at the nominal equilibrium distribution, using the existing robust or reconfiguration-based fault-tolerant control approaches are considered. The key idea is to temporarily maintain the process at an appropriate 'safe-park' distribution using the available depleted control action. This 'safe-park' distribution is chosen to prevent onset of hazardous situations as well ensure smooth resumption of nominal operation upon fault-repair. Utilizing the stability region characterization provided by the developed predictive controller, safe-park distributions from the safe-park candidates (equilibrium distributions subject to failed actuators) are chosen to preserve closed–loop stability upon fault repair. The proposed framework is illustrated on a diffusion-reaction process.

Finally in chapter 5, we review the presented results and discuss some future directions.

Chapter 2

Enhanced Stability Regions for Model Predictive Control of Nonlinear Process Systems

2.1 Introduction

The operation and control of chemical processes often encounters constraints that arise out of physical limitations on the control actuators. The constraints, if not accounted for in the control design, can cause performance deterioration or even instability in the closed–loop system. Specifically, the presence of constraints limits the set of initial conditions from where a process can be stabilized at a desired equilibrium point (the so-called null controllable region). A meaningful measure of how well the available control effort is being utilized by the control law can be obtained via a comparison of the stability region under a given control law with the null controllable region. Such a measure also provides assurance on the ability of the control law in recovering from the effect of disturbances that may temporarily drive the process away from the nominal operating point. These considerations have motivated extensive research on accounting for constraints via modifications in existing

control approaches (e.g., anti-windup designs [42]) as well as fostered the development of controllers that explicitly account for the presence of constraints via Lyapunov-based (see, for example, [48; 79; 41; 27; 28; 57] and [10; 16] for excellent reviews) and model-predictive control designs (see, for example, [63; 67; 1; 80; 76; 70; 82; 47] and the survey paper, [54]).

Given that process dynamics are sometimes identified or approximated by linear process systems, extensive research work has focused on designing and analyzing controllers that utilize a linear process description in computing the control action. Characterization of the null controllable region for linear process systems, while being difficult, is a tractable problem and has been the focus of several research efforts [46; 38; 78; 40]. Furthermore, several controller designs have been proposed that allow the possibility of turning any given *subset* of the null controllable region into the stability region of a proposed controller design [11; 12; 37]. Model predictive control (MPC) approaches allows implementation of stability constraints demanding the state to go to some invariant neighborhood of the origin (or the origin itself) [63; 12]. When guaranteeing feasibility from a subset of the null controllable region (under the assumption of initial feasibility of the optimization problem), the results use the approach of quantifying (and using as the horizon) the maximum over the minimum possible time for every point in the given set to be driven to the origin. Such an approach leads to prohibitively large values of the horizon (leading to practically un-implementable controllers) when requiring enhancement in the stability region. For some classes of linear systems (systems with real eigenvalues, low order systems with complex eigenvalues), explicit expressions for the boundary of the null controllable region, parameterized by the magnitude of input constraints, have recently been characterized [40]. The work in [40], however does not consider the problem of determining the control law that can stabilize all initial conditions in the null controllable region. As a special case of the key idea in the proposed work in this chapter, we show how the characterization developed in [40] can be utilized within the model predictive control framework to achieve stabilization from all initial conditions in the null controllable region, without unduly increasing the computation complexity of the optimization problem.

For nonlinear processes, the problem of explicitly characterizing the null controllable region

remains intractable. Lyapunov-based control designs address the problem of explicit characterizations of the stability region (see, e.g., [48; 27; 28]) under given control laws. The stability regions, however, are limited to (possibly conservative estimates of) invariant subsets (Ω) of the set of states for which the Lyapunov function (V) can be made to decay (Π) under the specific control law. In the model predictive control framework, several designs have been proposed that guarantee closed–loop stability contingent on the assumption of initial feasibility of the optimization problem [77; 50; 85; 75; 44; 70; 73; 64; 49; 7]. In [81; 82; 83] the optimization problem is reformulated within the framework of solving linear matrix inequalities (LMIs), with the ensuring 'error' due to local linearization accounted for via robust MPC formulation, and stability is guaranteed under the assumption of existence of a solution to the LMIs. In [31], Lyapunov-based and model predictive approaches were utilized within a switched controller framework to enable implementation of existing model predictive controllers with guaranteed stability region. More recently, in [58; 59] (see [16] for further results and references), the stability properties of auxiliary Lyapunov-based controllers of [48; 28] were utilized in formulating stability constraints in the optimization problem in a way that the predictive controllers of [58; 59] mimic the (possibly conservative) stability region of the auxiliary control designs. The stability region estimates in the existing designs [58; 59], however, do not fully utilize the constraint handling properties of the predictive controller approach to expand on the set of initial conditions from where closed–loop stability can be achieved.

Motivated by these considerations, this chapter considers the problem of control of nonlinear process systems subject to input constraints and presents predictive controllers that utilize control law independent analysis of the process dynamics in the controller design. First, linear process systems are considered and a predictive controller is designed that achieves closed–loop stability for every initial condition in the null controllable region (not just subsets of the null controllable region) without resorting to (practically) infinite horizon. For nonlinear process systems, the set of initial conditions for which $\dot{V} < 0$ is achievable (subject to constraints, and independent of the control law) is first characterized. This characterization is then utilized to formulate constraints in the predictive controller that not only require the Lyapunov function value to decay, but also require the process to

continue to evolve in the region from where successive decay in the Lyapunov function value is achievable. The enhancement in the set of initial conditions from where stability is achieved by the proposed method is illustrated using a chemical reactor example and the robustness with respect to parametric uncertainty and disturbances demonstrated via a styrene polymerization process.

2.2 Preliminaries

In this section, we present the process description, a polymerization reactor to motivate our results and review existing Lyapunov-based predictive control designs.

2.2.1 Process description

We consider nonlinear processes with input constraints, described by:

$$\begin{aligned} \dot{x} &= f(x) + G(x)u(t) \\ u &\in \mathcal{U} \end{aligned} \tag{2.1}$$

where $x \in \mathbb{R}^n$ denotes the vector of state variables, $u \in \mathbb{R}^m$ denotes the manipulated inputs taking values in a nonempty convex subset $\mathcal{U}$ of $\mathbb{R}^m$, where $\mathcal{U} = \{u \in \mathbb{R}^m : u_{min} \leq u \leq u_{max}\}$, $u_{min} \in \mathbb{R}^m$ and $u_{max} \in \mathbb{R}^m$ denote the lower and upper bounds on the manipulated input, $u^{norm} > 0$ is such that $\|u\| \leq u^{norm}$ implies $u \in \mathcal{U}$, where $\|\cdot\|$ is the Euclidean norm of a vector, and $f(0) = 0$. The vector function $f(x)$ and the matrix $G(x) = [g_1(x) \cdots g_m(x)]$ are assumed to be sufficiently smooth on their domains of definition. The notation $L_f h$ denotes the standard Lie derivative of a scalar function $h(\cdot)$ with respect to the vector function $f(\cdot)$, ∂X denotes the boundary of a set X and $x(T^+)$ is used to denote the limit of the trajectory $x(t)$ as T is approached from the right, i.e., $x(T^+) = \lim_{t \to T^+} x(t)$. Throughout the chapter, we assume that for any $u \in \mathcal{U}$ the solution of the system of Eq.2.1 exists and is continuous for all t. In the remaining of this section, we first present a styrene polymerization process that we will use to motivate our results and then review a Lyapunov-based model predictive control design that mimics the stability region of Lyapunov-based nonlinear control designs.

2.2.2 Motivating example

To motivate our predictive control design methodology and to demonstrate an application of our results, we introduce in this section a polystyrene polymerization process. To this end, consider a model for polystyrene polymerization process given in [39] (also studied in, e.g., [69])

$$\begin{aligned}
\dot{C}_I &= \frac{(F_i C_{If} - F_t C_I)}{V_{pr}} - k_d C_I \\
\dot{C_M} &= \frac{(F_m C_{Mf} - F_t C_M)}{V_{pr}} - k_p C_M C_P \\
\dot{T} &= \frac{F_t(T_f - T)}{V_{pr}} + \frac{(-\Delta H)}{\rho c_p} k_p C_M C_P - \frac{hA}{\rho c_p V}(T - T_c) \\
\dot{T}_c &= \frac{F_c(T_{cf} - T_c)}{V_c} + \frac{hA}{\rho_c C_{pc} V_c}(T - T_c) \\
C_P &= \left[\frac{2fk_d C_I}{k_t}\right]^{\frac{1}{2}} \\
k_d &= A_d e^{\frac{-E_d}{RT}} \\
k_p &= A_p e^{\frac{-E_p}{RT}} \\
k_t &= A_t e^{\frac{-E_t}{RT}}
\end{aligned} \tag{2.2}$$

where C_I, C_{If}, C_M, C_{Mf}, refer to the concentrations of the initiator and monomer in the inlet stream and in the reactor, respectively, T and T_f refer to the reactor and inlet stream temperatures and T_c and T_{cf} refer to the coolant inlet and jacket temperatures, respectively. The primary manipulated inputs are the monomer F_m and coolant F_c flow rates. As is the practice with the operation of the polystyrene polymerization process [39], the solvent flow rate is also changed in proportion to the monomer flow rate. The values of the process parameters are given in Table 2.2. The control objective is to stabilize the reactor at the unstable equilibrium point ($C_i = 0.0480\ kmolm^{-3}$, $C_M = 2.3331\ kmolm^{-3}$, $T = 354.92\ K$, $T_c = 316.2429\ K$), corresponding to the nominal values of the manipulated inputs of $F_c = 0.000131 m^3 s^{-1}$ and $F_m = 0.000105 m^3 s^{-1}$. The manipulated inputs are constrained as $0 \leq F_m \leq 0.003105\ m^3 s^{-1}$, $0 \leq F_c \leq 0.0031\ m^3 s^{-1}$. Owing to the high dimensionality and nonlinearity of the process (as will be subsequently seen), stability region estimates

derived using Lyapunov-based tools are conservative and development of control designs that best use the available control action to enhance the set of initial conditions from where stabilization is achieved is of significance. We will demonstrate the application, as well as investigate the robustness, of the proposed control design to the styrene polymerization example, while illustrating the finer details of the proposed controller using an illustrative chemical reactor.

2.2.3 Lyapunov-based model predictive control

In this section, we briefly review a recent result on a Lyapunov-based predictive controller that has an explicitly characterized feasibility and stability region. To this end, consider the system of Eq.2.1, for which a predictive controller [58] is designed of the form:

$$u_{LBPC} = argmin\{J(x,t,u(\cdot))|u(\cdot) \in S\} \tag{2.3}$$

$$s.t.\ \dot{x} = f(x) + G(x)u \tag{2.4}$$

$$\dot{V}(x(\tau)) \leq -\epsilon^* \ \forall\, \tau \in [t, t+\Delta)\ if\ \ V(x(t)) > \delta^{'} \tag{2.5}$$

$$V(x(\tau)) \leq \delta^{'}\ \forall\, \tau \in [t, t+\Delta)\ \ if\ \ V(x(t)) \leq \delta^{'} \tag{2.6}$$

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.2.4 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 $u(\tau) = u[j]$ for all $\tau \in [t+j\Delta, t+(j+1)\Delta)$. The performance index is given by

$$J(x,t,u(\cdot)) = \int_t^{t+T} \left[\|x^u(s;x,t)\|_Q^2 + \|u(s)\|_R^2\right] ds \tag{2.7}$$

where Q is a positive semi-definite symmetric matrix and R is a strictly positive definite symmetric matrix. $x^u(s;x,t)$ denotes the solution of Eq.2.1, due to control u, with initial state x at time t. The minimizing control $u^0(\cdot) \in S$ 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 of the form (e.g., see [48; 27; 28]):

$$u(x) = -k(x)(L_G V)'(x) \tag{2.8}$$

$$k(x) = \frac{L_f V(x) + \sqrt{(L_f V(x))^2 + (u_{max}\|(L_G V)'(x)\|)^4}}{\|(L_G V)'(x)\|^2 \left[1 + \sqrt{1 + (u_{max}\|(L_G V)'(x)\|)^2}\right]} \tag{2.9}$$

when $L_G V(x) \neq 0$ and $k(x) = 0$ when $L_G V(x) = 0$ where $L_f V(x) = \dfrac{\partial V(x)}{\partial x} f(x)$, $L_G V(x) = [L_{g_1} V(x) \cdots L_{g_m} V(x)]'$ and $g_i(x)$ is the i-th column of the matrix $G(x)$. For the controller of Eqs.2.8–2.9, one can show, using a standard Lyapunov argument, that whenever the closed–loop state, x, evolves within the region described by the set:

$$\Pi = \{x \in \mathbb{R}^n : L_f V(x) \leq u^{norm}\|(L_G V)'(x)\|\} \tag{2.10}$$

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.,

$$\Omega = \{x \in \mathbb{R}^n : V(x) \leq c^{max}\} \tag{2.11}$$

where $c^{max} > 0$ is the largest number for which $\Omega \subseteq \Pi$. Closed–loop stability and feasibility properties under the Lyapunov–based predictive controller are inherited from the bounded controller under discrete implementation and are formalized in Theorem 2.1 below (for a proof, see [58]).

Theorem 2.1 [58]: *Consider the constrained system of Eq.2.1 under the MPC law of Eqs.2.3–2.7. Then, given any $d \geq 0$, $x_0 \in \Omega$, where Ω was defined in Eq.2.11, there exist positive real numbers δ', ϵ^*, Δ^*, such that if $\Delta \in (0, \Delta^*]$, then the optimization problem of Eq.2.3-2.7 is feasible for all times, $x(t) \in \Omega$ for all $t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d$.*

Remark 2.1: 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. The analysis of discrete implementation of the control law of Eqs.2.8–2.9 ensures

the existence of a feasible solution to the predictive controller formulation from an explicitly characterized set of initial conditions. While the predictive controller utilizes the auxiliary control design to address the problem of guaranteeing initial feasibility, utilization of the constraint of Eq.2.5 only imitates the stability properties (and the stability region) of the bounded controller and does not fully exploit the constraint handling capabilities of the predictive control approach to expand on the set of initial conditions from where closed–loop stability is achieved.

2.3 Enhancing the stability region estimates using model predictive control

The stability region estimates of existing Lyapunov-based predictive controllers are limited (and dependent upon) stability region estimates obtained using the auxiliary control approaches, and by not fully utilizing the constraint handling capabilities of the predictive control approach, suffer from the same possible conservatism as the auxiliary control designs. In this section, we present a predictive control design wherein constraints are formulated that, by better utilizing Lyapunov-based analysis tools, enhance the set of initial conditions from where closed–loop stability is achieved. Before we proceed to the controller design for nonlinear systems, we first consider, as a special case, linear systems subject to constraints and show how the utilization of the process dynamics in the controller design results in a predictive controller that guarantees stabilization from all initial conditions for which closed–loop stability can be achieved subject to constraints. We next consider nonlinear systems and formulate a predictive controller that not only provides an explicit characterization of the stability region but also enhances the set of initial conditions from which closed–loop stability is achieved.

2.3.1 Linear systems subject to constraints

Linear descriptions of the process dynamics are often utilized in controller design for chemical processes. While extensive results exist on constructing control designs that guarantee stability from any given subset of the null controllable region (see, e.g., [46; 38; 78; 40; 11; 12; 37; 63; 12; 6]), the computational complexity of the control design typically renders the control implementation impractical as larger and larger stability regions are desired. Furthermore, there exists a lack of theoretical results that guarantee stability for any initial condition in the entire null controllable region. In this section, we show how the characterization of the null controllable region, developed in [40], can be utilized within the predictive control approach in achieving stability for all initial conditions in the null controllable region. To this end, consider processes whose dynamics can be described by

$$\dot{x}(t) = Ax(t) + Bu(t),\ u \in \mathcal{U} \tag{2.12}$$

where A and B are constant $n \times n$ and $n \times m$ matrices respectively. A summary of characterization of the null controllable region is described below [40].

2.3.1.1 Null controllable region for linear systems

A state x_0 is said to be null controllable if there exists a $T \in [0, \infty)$ and an admissible control $u(t)$ such that the state trajectory $x(t)$ of the system of Eq.2.12 satisfies $x(0) = x_0$ and $x(T) = 0$. The union of all null controllable states is called the null controllable region of the system which we denote by X^{max}. The null controllable region characterized as (see [40]) $X^{max} = \bigcup_{T \in [0,\infty)} \{x = -\int_0^T e^{-A\tau} B u(\tau) d\tau : u(\tau) \in \mathcal{U}\}$ can be shown to be a bounded convex open set containing the origin if A is unstable. It can be shown that the null controllable region of the multi-input system of Eq.2.12 is the Minkowski sum of the null-controllable regions of the single input subsystems

$$\dot{x}(t) = Ax(t) + b_i u_i(t),\ u_i(t) \in \mathcal{U}_i \tag{2.13}$$

where $B = [b_1\ b_2\ \ldots b_m]$ and u_i denotes the ith component of the vector u. Specifically, let X_i^{max} denote the null controllable region of the subsystem of Eq.2.13 then $X^{max} = \sum_{i=1}^{m} X_i^{max} = \{x_1 + x_2 + \cdots + x_m : x_i \in X_i^{max}, i = 1, \ldots, m\}$. For systems with real eigenvalues (see [40] for computing the null controllable region for low dimensional systems with complex eigenvalues), the boundary of the null controllable region can be computed as [40]

$$\partial X_i^{max} = \{\pm[\sum_{j=1}^{n-1} 2(-1)^j e^{-A(t-t_j)} + -1^n I]A^{-1}b_i u_i^{norm} : 0 = t_1 \leq t_2 \leq \cdots \leq t_{n-1} \leq t \leq \infty\} \tag{2.14}$$

Eq.2.14 can be used to verify whether a state lies within the null controllable region and, more importantly, can be used to compute, for a given state, the unique value of u_i^* such that the state resides on the boundary of the null controllable region of a system of the form of Eq.2.13 with a constraint of u_i^* on the manipulated input u_i. Utilizing these properties, for a given state x_0 we define a function $\bar{u}_i^*(x_0)$ as the unique positive number u_i^* for which $x_0 \in \partial X_i^{max}(u_i^*)$. Essentially, for a given state x_0, Eq.2.14 is solved to yield t_i, $i = 2 \ldots n-1$, t and u_i^{norm}. The value of u_i^{norm} equals the fictitious constraint u_i^* (see Eq.2.22 for an illustrative example). In the next subsection, we show how the predictive control approach can utilize such a characterization in enabling stabilization from all points within the null controllable region.

2.3.1.2 Predictive control design with the null controllable region as the stability region

The key idea in the predictive control design is as follows: for any given value of the state, the value u_i^* represents the minimum control action required to stabilize the system. A meaningful control action therefore would be one that drives the process in a way that the minimum control action required to stabilize the system decreases. This intuitive idea is formulated mathematically in Theorem 2.2 below. To this end, consider the system of Eq.2.12 and an $x_0 \in X^{max}$. Let $x_{i,0} \in X_i^{max}(u_i^*)$, $i = 1, \ldots, m$ be such that $x_0 = \sum_{i=1}^{m} x_{i,0}$, with $u_i^* \leq u_i^{norm}$. The predictive controller that guarantees stabilization from all initial

conditions in X^{max} is of the form:

$$u_{i,MPC} = argmin\{J(x,t,u(\cdot))|u(\cdot) \in U,\ x(0) = x_{i,0}\} \tag{2.15}$$

$$s.t.\ \dot{x} = Ax + b_i u_i \tag{2.16}$$

$$\dot{\bar{u}}_i^*(x(t)) \leq 0 \tag{2.17}$$

Eq.2.16 is the linear model describing the time evolution of the state x, due to the *ith* manipulated input. The performance index is given by

$$J(x,t,u(\cdot)) = \dot{\bar{u}}^*(x_i(t)) \tag{2.18}$$

The minimizing controls $u_i^0(\cdot)$ are then applied to the plant and the procedure is repeated indefinitely. Note that the above formulation is a continuous time version of the MPC, and assumes instantaneous evaluation and implementation of the computed control value. The result under continuous implementation is presented in Theorem 2.2 below, and the 'implement and hold' approach demonstrated and discussed in the simulation example for linear systems and addressed explicitly in the predictive control design for nonlinear process systems in Theorem 2.3.

Theorem 2.2 : *Consider the constrained system of Eq.2.12 under the MPC law of Eqs.2.15–2.18. Then, given any $x_0 \in X^{max}$, the optimization problem of Eq.2.15-2.18 is feasible for all times, and $\lim_{t\to\infty} x(t) = 0$.*

Proof of Theorem 2.2: We first prove the results for a single input system, and then illustrate the generalization to multi-input systems. In the proof, the key things to show are guaranteed feasibility of the optimization problem and the optimal solution leading to closed–loop stability.

Single input system: In this part of the proof, we will drop the subscript on the input with the understanding that a single input system is being analyzed. Consider an $x_0 \in X^{max}$, for which $\bar{u}^*(x_0) = u_0^* < u^{norm}$. In part 1, we show feasibility of the optimization problem, and in part 2, the implementation of the optimal solution resulting in closed–loop stability.

Part 1: Since $x_0 \in X^{max}(u^{norm})$, there exists at least one input trajectory $u(t)$ with $|u(t)| \leq u^{norm}$ such that $\lim_{t\to\infty} x(t) = 0$. Out of all such possible trajectories (for which

$\lim_{t\to\infty} x(t) = 0$) let

$$u_1^* = \min_{|u_1(t)|\leq u^{norm}} \max_t \bar{u}^*(x_{u_1}(t)) \tag{2.19}$$

where $x_{u_1}(t)$ denotes the state profile corresponding to an input profile of $u_1(t)$. Thus u_1^* represents the minimum (over all possible stabilizing trajectories) of the maximum (over time) value that the function $\bar{u}^*(\cdot)$ takes. Note that if $u_1^* \geq u^{norm}$ then an x_1^* such that $\bar{u}^*(x_1^*) = u_1^*$ will be such that $x_1^* \in X^{max}(u^{norm})$ (in other words, it would mean that the process starting from a state outside the null controllable region is actually stabilized) which leads to a contradiction, we therefore have that

$$u_1^* < u^{norm} \tag{2.20}$$

Let $u_1^* = u_0^* + \gamma$ with $\gamma > 0$. Since $x_0 \in \partial X^{max}(u_0^*)$, this implies that $x_0 \in X^{max}(u_0^* + \gamma/2)$. Denoting

$$u_2^* = \min_{|u_2(t)|\leq u_0^*+\gamma/2\, t,\, x(0)=x_0} \max \bar{u}^*(x_{u_2}(t)) \tag{2.21}$$

and invoking Eq.2.20 again with $u_0^* + \gamma/2 = u^{norm}$, we get that $u_2^* < u_0^* + \gamma/2$. Furthermore, noting that the minimizations of Eq.2.19 and Eq.2.21 are exactly the same, albeit with a larger constraint in Eq.2.19 compared to Eq.2.21, we get that $u_1^* = u_0^* + \gamma \leq u_2^* < u_0^* + \gamma/2$, which once again leads to a contradiction, implying γ cannot be a positive real number. This finally leads to the conclusion that for any $x_0 \in X^{max}(u^{norm})$, there exists a manipulated input profile and corresponding state trajectory such that $\bar{u}^*(x(t+\delta t)) \leq \bar{u}^*(x(t))$ for all $\delta t > 0$. This implies that along such a trajectory the function $\bar{u}^*(x(\cdot))$ is non-increasing, implying the feasibility of the constraint $\dot{\bar{u}}^*(x(t)) \leq 0$.

Part 2: Having established the feasibility of the optimization problem in Part 1 above, consider now an x_0 in X^{max} for which $J^*(x_0, t, u(\cdot)) = \min \dot{\bar{u}}^*(x_0(t)) = 0$. This implies that for this x_0, the minimizing u_{MPC} is such that the vector $Ax_0 + bu$ (which represents the current direction of the state trajectory) is on the tangent plane to the surface defining $\partial X^{max}(\bar{u}^*(x_0))$. This would further imply that the vectors Ax_0 and bu_{MPC} must themselves be co-planar (if they were not, a different allowable value for u_{MPC} could have been chosen to point the vector $Ax_0 + bu$ away from the tangent plane to the surface defining $\partial X^{max}(\bar{u}^*(x_0))$, resulting in a $J^*(x_0(t)) < 0$). Upon implementation of such a u_{MPC}, the

tangent to ∂X^{max} at $x(t^+)$ cannot remain in the same plane (due to the strict convexity of the boundary of the set X^{max}) as that of the vector b resulting in $\min \dot{\bar{u}}^*(x_0^+) < 0$. Therefore, for any x_0 for which the minimum of $\dot{\bar{u}}^*(x(0)) = 0$, the minimum of $\dot{\bar{u}}^*(x(0^+)) < 0$ ensuring convergence of $\bar{u}^*(x(t))$ to zero, in turn resulting in $\lim_{t\to\infty} x(t) = 0$.

Multiple input system: The result for the multiple input system is a direct generalization for the single input system. Having defined $x_0 = \sum_{i=1}^{m} x_{i,0}$, X^{max} and X_i^{max}, the evolution of the multiple input system is exactly the same as the sum of the multiple single input systems. Feasibility and stability of the subsystems yields stability for the original multi-input system. □

Remark 2.2: While extensive results exist on stabilization of linear systems, the stability guarantees are provided for subsets (which can get arbitrarily close to the null controllable region) of the null controllable region, and the control design becomes practically impossible to implement as larger stability regions are sought. The approach in the existing results is to estimate the time that it would take for all initial conditions in the 'desired' stability region to reach the origin and to incorporate it in some fashion in the controller design. In model predictive control approaches, this idea can directly be utilized via large or variable horizon (e.g., see [63; 12]), leading to computationally expensive optimization problems. In all of these approaches, the idea remains the same: require the state to go to the origin (or some neighborhood of the origin) by some time (the horizon) and pick a large enough horizon to ensure feasibility of the optimization problem. When the horizon is variable, the optimization problem is in general difficult to solve since the number of decision variables in the optimization problem itself keep changing. When the horizon is fixed, the number of decision variables that have to be retained grows as larger and larger subsets of the null controllable region are desired as the stability region. Note that in our result, feasibility from the null controllable region is achieved via appropriate formulation of the stability constraint, and existing predictive controllers, which assume initial feasibility of the optimization problem, are not guaranteed to be feasible from all initial conditions in the null controllable region. In contrast, the proposed predictive controller achieves guaranteed feasibility and stability for all initial conditions in the null controllable region.

Note also that while the specific objective function of Eq.2.18 is designed to satisfy the overriding requirement of stabilization (especially for initial conditions close to the boundary of the null-controllable region for which existing predictive control designs would result in a computationally un-implementable controller), once the state trajectory reaches closer to the desired equilibrium point (and inside the stability region of existing predictive controllers [58]), switching can be executed to implement the predictive controllers that allow for the minimization of a more general objective function.

Remark 2.3: Note that while the results of Theorem 2.2 are derived under the assumption of continuous implementation of the control action, in practice the results can be implemented when the control action is computed and held for a certain period of time (as in most applications). In doing so, for any given value of the state the current value of u_i^* is computed, and instead of computing a control action that yields $\dot{u}_i^* < 0$, a control action is computed that results in a lower value of u_i^* at the next sampling instant (see the simulation example for a demonstration) thereby not requiring the computation and satisfaction of the constraint on the derivative of u_i^*.

Remark 2.4: The result achieving stabilization from the null controllable region can best be understood in light of the result using the control Lyapunov function. Specifically, the controller of Eqs.2.3–2.18 does not guarantee stabilization from all initial conditions in the null controllable region due to the following reasons: (1) for a choice of a CLF V, $\dot{V}$ is not necessarily guaranteed to be negative for all initial conditions in X^{max}, (2) even if a certain choice of the CLF resulted in $\dot{V}$ being negative for all initial conditions in X^{max}, the level sets of a CLF may not necessarily coincide with the boundary of the null controllable region. The stability region estimate would therefore typically be a subset of the null controllable region.

2.3.1.3 Simulation example

Consider a linear system of the form of Eq.2.12 with $A = \begin{bmatrix} 0 & -0.5 \\ 1.0 & 1.5 \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ -1.0 \end{bmatrix}$ and $u^{norm} = 1$ (representing a nominally unstable linear system). The null controllable region, X^{max}, for this system is computed using Eq.2.14 and is shown in Fig.2.1. For the sake of comparison, the stability region for the predictive controller of Theorem 2.1, computed using a quadratic Lyapunov function, the set Π (as described in Eq.2.10) and then constructing the largest level set of the Lyapunov function $V(x) = c^{max} = 1.1$ completely contained in Π is also shown, denoted by Ω. The conservativeness in using level sets of the Lyapunov function to estimate the stability region (for this particular example) is seen via the part of X^{max} not captured in Ω. While the theoretical results are derived under the assumption of continuous implementation of the control action, the simulation results demonstrate the discrete implementation of the controller, with a discretization time of $\Delta = 0.1$. The constraint of Eq.2.17 is therefore implemented as $\bar{u}^*(x(t+\Delta)) \leq \bar{u}^*(x(t))$. The function $\bar{u}^*(x)$ is evaluated by computing the unique solution pair u^*, T to the equation (utilizing Eq.19 in [40]):

$$x(t) = (2e^{AT} + I)A^{-1}Bu^* \tag{2.22}$$

and then by evaluating $\bar{u}^*(\cdot) = |u^*|$. Note that the same equation, setting $u^* = 1$, and by varying T from 0 to a sufficiently large number, is used to construct the boundary of the set X^{max} (for more details, see [40]). The optimization problem in the predictive controller formulation is solved by using the MATLAB function FMINCON.

To illustrate the stabilization properties of the proposed predictive controller, we pick an initial condition $x_0 = [-0.6032,\ 0.6003]$ in X^{max} and try to stabilize it using the predictive controller of Eqs.2.3–2.5 (that requires the control action to result in a decay in the value of $V(x)$). As can be seen from the dashed lines in Fig.2.1, closed–loop stability is not achieved (the corresponding state trajectories and input profile can be seen as dashed lines in Fig.2.2 (a-c)). In contrast, when the control action computed by the proposed predictive controller is implemented, closed–loop stability is achieved. Note that the proposed predictive controller does not try to compute a control action that decreases the value of the Lyapunov

function, but instead computes a control action that drives the state trajectory along lower 'level sets' of u^*. Fig.2.2 (d-e) shows the evolution of the Lyapunov function and that of $\bar{u}^*(x(t))$ for the two scenarios. Once again, the figures demonstrate the decrease in the value of the Lyapunov function initially achievable (see inset), after which the state escapes the set of initial conditions from where the negative definiteness of $\dot{V}$ can be enforced. In contrast, the solid lines show the decrease in the value of $\bar{u}^*(x(t))$ enforced by the predictive controller (note that the predictive controller also enforces a continual decrease in the value of the Lyapunov function is only incidental). In summary, the proposed predictive controller drives the state trajectory to successively lower values of $\bar{u}^*(x(t))$ eventually stabilizing the system.

2.3.2 Model predictive control of nonlinear systems

In contrast to linear systems, where an explicit characterization of the null controllable region is possible, for nonlinear process systems such a characterization remains an open problem. In [59], predictive controllers were designed that utilized auxiliary Lyapunov–based control design for estimating the feasibility and stability region. In the predictive control design of [59], the first layer of conservativeness stems from the estimation of Π which only captures initial conditions for which negative definiteness of $\dot{V}$ can be achieved by the auxiliary control law, instead of characterizing the set of initial conditions for which negative definiteness of $\dot{V}$ can be achieved independent of the control law (which we will characterize and denote by Π^+). Additionally, only requiring $\dot{V}$ to be negative allows stabilization from all initial conditions inside Ω but misses out on achieving stabilization from initial conditions outside Ω but inside Π.

2.3.2.1 Nonlinear model predictive controller

We utilize in this section the constraint handling capabilities of the predictive controller to expand on the set of initial conditions from where closed–loop stability can be achieved to alleviate the possible conservatism associated with Lyapunov-based control designs. To this

cnd, we first characterize the set Π^+ for which negative definiteness of the Lyapunov function derivative can be achieved subject to manipulated input constraints (and independent of the control law) described by

$$\Pi^+ = \{x \in \mathbb{R}^n : L_f V(x) + \sum_{i=1}^{m} L_{G_i^{min}} V(x) u^i \leq -\epsilon^{**}\} \tag{2.23}$$

where $L_{G_i^{min}} V(x) u^i = L_{G_i} V(x) u^i_{max}$ if $L_{G_i} V(x) \leq 0$ and $L_{G_i^{min}} V(x) u^i = L_{G_i} V(x) u^i_{min}$ if $L_{G_i} V(x) > 0$ and ϵ^{**} is a positive number to be defined. The set Π^+ therefore denotes the entire set of initial conditions from where $\dot{V} < -\epsilon^{**}$ is achievable (and not just the set from where a specific control law can achieve $\dot{V} < 0$ thereby improving upon the estimate Π in Eq.2.10). The idea behind the expression in Eq.2.23 is as follows: each element of the vector $L_G V(x)$, denoted by $L_{g_i} V(x)$ captures the effect of the *ith* component of the manipulated input on the Lyapunov function derivative. The term $L_{G_i^{min}} V(x) u^i$ therefore captures the most that the *ith* manipulated input can contribute towards making $\dot{V}(x)$ negative. Alternatively, the expression can also be thought of as the set of states for which $\dot{V}(x)$ is negative under the 'bang-bang' control law given by $u_i(x) = -sgn(L_{g_i} V(x)) u_i^{norm}$ (for the case where $|u^i_{max}| = |u^i_{min}| = u_i^{norm}$) where $sgn(x) = 1$ if $x \geq 0$ and $sgn(x) = -1$ if $x < 0$. By accounting for the maximum control action available, the set Π^+ expands on the estimate Π. Subsequently, computation of the largest level set Ω^+, of the form

$$\Omega^+ = \{x \in \mathbb{R}^n : V(x) \leq c^{max^+}\} \tag{2.24}$$

completely contained in Π^+ improves upon the estimate Ω. Requiring $\dot{V} \leq -\epsilon^{**}$ instead of only requiring $\dot{V} < 0$ is formulated to ensure stabilization subject to implement and hold (similar to the result in Theorem 2.1). Having defined the sets Π^+ and Ω^+ the predictive controller enhancing the set of initial conditions from which stability is achieved (accounting specifically for initial conditions outside Ω^+ but inside Π^+) takes the form:

$$u = argmin\{J(x, t, u(\cdot)) | u(\cdot) \in S\} \tag{2.25}$$

$$s.t.\ \dot{x} = f(x) + G(x)u \tag{2.26}$$

$$\dot{V}(x(\tau)) \leq -\epsilon^* \ \forall \tau \in [t, t+\Delta) \ if \ \ V(x(t)) > \delta' \tag{2.27}$$

$$V(x(\tau)) \leq \delta' \ \forall \tau \in [t, t+\Delta) \ \ if \ \ V(x(t)) \leq \delta' \tag{2.28}$$

$$x(t+\tau) \ \in \ \Pi^+ \ \forall \tau \in [t, t+\Delta) \ if \ \ V(x(t)) > c^{max^+} \tag{2.29}$$

where $S = S(t,T)$ is the family of piecewise constant functions (functions continuous from the right), with period Δ, mapping $[t, t+T]$ into U and T is the horizon. Eq.2.26 is the model describing the time evolution of the state x under continuous operation, V is the control Lyapunov function (CLF) and δ', $\epsilon^* > 0$ are parameters defined in Theorem 2.1. The performance index is given by

$$J(x, t, u(\cdot)) \ = \ \int_t^{t+T} \left[\|x^u(s; x, t)\|_Q^2 + \|u(s)\|_R^2 \right] ds \tag{2.30}$$

where Q is a positive semi-definite symmetric matrix, R is a strictly positive definite symmetric matrix. $x^u(s; x, t)$ denotes the solution of Eq.2.1, due to control u, with initial state x at time t. The minimizing control $u^0(\cdot) \in S$ is then applied to the process over the interval $[t, t+\Delta)$ and the procedure is repeated indefinitely. The feasibility and stability properties of the predictive controller are formalized in Theorem 2.3 below:

Theorem 2.3 : *Consider the constrained system of Eq.2.1 under the MPC law of Eqs.2.25–2.30. Then, given any $d > 0$, there exists a positive real number ϵ^{**} such that if $x_0 \in \Omega^+$, where Ω^+ was defined in Eq.2.24, then the optimization problem of Eq.2.25-2.30 is guaranteed to be feasible for all times, $x(t) \in \Omega^+$ for all $t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d$. Furthermore, for $x_0 \in \Pi^+ \backslash \Omega^+$ where Π^+ was defined in Eq.2.23, if the optimization problem of Eq.2.25-2.30 is successively feasible for all times, then $x(t) \in \Pi^+ \bigcup \Omega^+$ for all $t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d$.*

Proof of Theorem 2.3: The proof of the theorem comprises of two parts. In part 1, we show the feasibility of the optimization problem for all $x \in \Omega^+$ and subsequent convergence to the desired neighborhood of the origin, while in part 2, for $x \notin \Omega^+$ we show convergence to the desired neighborhood of the origin upon assumption of feasibility of the optimization problem.

Part 1: From Theorem 2.1 and the proof (see [59]) it follows that given d, there exist positive real numbers δ' and Δ^* such that if $\Delta \in (0, \Delta^*]$ then satisfaction of the constraints

of Eqs.2.27-2.28 ensures convergence to the desired neighborhood of the origin. In the proof, we show the existence of the positive real number ϵ^{**} (yielding Ω^+) which ensures initial and continued satisfaction of the constraints of Eqs.2.27-2.28 for all $x_0 \in \Omega^+$. From the continuity of the functions $f(\cdot)$, $G(\cdot)$ $L_fV(\cdot)$ $L_GV(\cdot)$, the boundedness of u and by restricting the state x_0 to the set Ω^+, it follows that given ϵ^* and Δ^* there exists a positive real number ϵ^{**} such that if $L_fV(x_0)+L_GV(x_0)u_0 \leq -\epsilon^{**}$ then $L_fV(x(\tau))+L_GV(x(\tau))u_0 \leq -\epsilon^* \; \forall \; \tau \in (0, \Delta^*]$, where ϵ^*, Δ^* were defined in Theorem 2.1. This ensures initial feasibility of the constraints of Eq.2.27 for all $x_0 \in \Omega^+$. Initial satisfaction of the constraints ensures that $V(x(t+\Delta)) \leq V(x(t))$, which in turn implies that $x(t+\Delta) \in \Omega^+$ for all $t \geq 0$, thereby yielding successive feasibility of the optimization problem. Successive feasibility of the optimization problem leads to convergence to the desired neighborhood of the origin.

Part 2: For all $x_0 \notin \Omega$, the assumption of initial and successive feasibility of the constraint of Eq.2.29 ensures that $x(t+\tau) \in \Pi^+$ for all $x(t) \notin \Omega^+$, $\tau \in (0, \Delta^*]$. Also, the satisfaction of the constraint of Eq.2.27 ensures that the value of the Lyapunov function continues to decrease, implying that the state trajectory eventually converges to the set Ω^+. Convergence to $\limsup_{t \to \infty} \|x(t)\| \leq d$ follow from part 1 above. This concludes the proof of Theorem 2.3. □

Remark 2.5: The meaning and implication of the constraints of Eqs.2.27–2.29 is as follows: the constraint of Eq.2.27 requires the control action to enforce a decay in the value of the Lyapunov-function value over the next time interval; because of the discrete nature (implement and hold) of the control action, such decay may not be achievable for all state values, and is only requested to drive the process to a desired neighborhood of the origin defined by $V(x) \leq \delta'$. Once the process reaches the desired neighborhood of the origin, the constraint of Eq.2.28 prevents the state from escaping that neighborhood. For initial conditions within a level set of the Lyapunov function (Ω^+), successive decays in the Lyapunov function value is achievable and sufficient to drive the state to the desired neighborhood of the origin. For initial conditions outside the set Ω^+, the constraint of Eq.2.29 asks for the control action to be computed such that for the process state at the next time instant, negative definiteness of $\dot{V}$ can be successively achieved. This ensures

that out of all possible control actions that can achieve negative definiteness of $\dot{V}$, one is chosen that ensures that the state trajectory stays within Π^+ from where continued decay of the Lyapunov function value is possible. A continued decay in the Lyapunov function value leads to convergence to the desired neighborhood of the origin. Note also that in contrast to the result on linear system, guaranteed feasibility for all initial conditions in the null controllable region simply cannot be achieved, yet Eq.2.29 represents a constraint that at least guides the control law to take some meaningful control action for initial conditions outside Ω^+. This constraint goes beyond (and does better than) simply requiring a decay in the value of the Lyapunov function and enables stabilization from a larger set of initial conditions (see the simulation example for a demonstration).

Remark 2.6: Note that the estimates of the stability region, and the enhancement with the proposed predictive controllers are influenced by the choice of the control Lyapunov function. Furthermore, referring to the choice of the control Lyapunov function, it is important to note that a general procedure for the construction of CLFs for nonlinear process systems of the form of Eq.2.1 is currently not available. We refer the reader to [52] for further discussion on this issue.

Remark 2.7: Note that in this work, we rely on available nonlinear optimization solvers (e.g MATLABs FMINCON) to handle the optimization problem in Eqs.2.25–2.30. The ability to compute a local or global solution does not affect the stability results given in Theorem 2.3, and remains beyond the scope of the present work. We also note that the presence of multiple local optima can cause sudden rapid changes within the implemented input trajectory which may be undesirable in many applications. This behavior can be mitigated by including a weighted term on the movement of the computed input value within the objective function in Eq.2.30.

2.3.2.2 Illustrative chemical process example

Consider a continuous stirred tank reactor 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:

$$\begin{aligned} \dot{C}_A &= \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{RT_R}} C_A \\ \dot{T}_R &= \frac{F}{V}(T_{A0} - T_R) + \frac{(-\Delta H)}{\rho c_p} k_0 e^{\frac{-E}{RT_R}} C_A + \frac{Q}{\rho c_p V} \end{aligned} \tag{2.31}$$

where C_A denotes the concentration of the species A, T_R denotes the temperature of the reactor, Q is the heat added to 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 Table 2.1. The control objective is to stabilize the reactor at the unstable equilibrium point $(C_A^s,\ T_R^s) = (0.57\ Kmol/m^3, 395.3\ K)$ using the rate of heat input, Q, and change in inlet concentration of species A, $\Delta C_A = C_{A0} - C_{A0_s}$ as manipulated inputs with constraints: $|Q| \leq 32\ KJ/s$ and $|\Delta C_{A0}| \leq 1\ Kmol/m^3$.

We first construct a Lyapunov-based predictive controller using a $V(x) = x'Px$ where $x = (C_A - C_A^s,\ T_R - T_R^s)$, $P = \begin{pmatrix} 0.983 & 0.025 \\ 0.025 & 0.001 \end{pmatrix}$ where the matrix P is computed by solving the Riccati inequality with the linearized system matrices. The parameters in the objective function of Eq.2.30 are chosen as $Q = qI$, with $q = 0.1$, and $R = \begin{pmatrix} 10.0 & 0.0 \\ 0.0 & 10000.0 \end{pmatrix}$. The set Π and the stability region estimate under the Lyapunov-based controller Ω are computed and shown in Fig.2.3. Predicition and control horizons of 0.01 *min* are used in implementing the predictive controller. The constrained nonlinear optimization problem is solved using the MATLAB subroutine FMINCON, and the set of ODEs is integrated using the MATLAB solver ODE15s.

To illustrate the enhancement in the set of initial conditions from where closed–loop stability can be achieved using the proposed controller, we pick an initial condition $C_A(0)$, $T_R(0) = 1.113\ kmol/m^3$, $395.3\ K$ outside Ω^+ but inside Π^+. We first implement the Lyapunov-based predictive controller of Theorem 2.1 that only requires the value of the Lyapunov function to decrease. Since the initial condition is within the set Π^+, there exists a control action that can enforce negative definiteness of the Lyapunov function and the controller proceeds to implement such control action. However, enforcing negative definiteness of $\dot{V}$

(i.e., driving the trajectory to successively lower level curves of the Lyapunov function), is not sufficient to ensure that the trajectory remains within the set Π^+. At $t = 0.12$ min, the state trajectory escapes out of Π^+, and it is no longer possible to find a control action that enforces negative definiteness of $\dot{V}$. If the stability constraints are removed to allow feasibility of the optimization problem, the value of the Lyapunov function continues to increase (see dashed lines in Figs.2.4–2.5 for the corresponding state and input profiles), and closed–loop stability is not achieved. In contrast, if the proposed predictive controller is implemented, it not only enforces negative definiteness of $\dot{V}$, but also ensures that the state trajectory does not escape Π^+. In other words, out of possible state trajectories along decreasing values of the level curves of $V(x)$, those are chosen (if they exist) that keep the state profile in Π^+. Closed-loop stability is thereby achieved, demonstrating an expansion on the set of initial conditions from where closed–loop stability can be achieved by better utilizing the constraint enforcing capabilities of the predictive control approach.

2.4 Application to the styrene polymerization process

Having illustrated the enhancement in the stability region via a chemical reactor example, we implement the predictive controller on the styrene polymerization process. To this end, first a quadratic Lyapunov function of the form $V(x) = x^T P x$ with

$$P = \begin{bmatrix} 52570 & 2457 & 261.4 & 6.942 \\ 2457 & 181.9 & 13.40 & 2.561 \\ 261.4 & 1.340 & 1.708 & 0.2300 \\ 6.942 & 2.561 & 0.2300 & 0.9668 \end{bmatrix}$$

is chosen in the predictive controller design and the set of initial conditions from where $\dot{V} < 0$ is achievable (the set Π^+) and the invariant set Ω^+ within Π^+ (defined by $V(x) \leq 105$) is computed. In the application, the 'discretized' version of the stability constraint are implemented, i.e., $V(x(t+\Delta)) < V(x(t))$ is implemented instead of $\dot{V}(x(t+\tau)) < -\epsilon^*$, and $x(t+\Delta) \in \Pi^+$ is implemented instead of $x(t+\tau) \in \Pi^+$, where a sampling time $\Delta = 5min$ is used. The weighting matrices in the predictive controller were chosen as $Q = qI_x$ with

$q = 0.1$ and $R = rI_u$ with $r = 1$, where I_x and I_u are the identity matrices of appropriate dimensions.

We first demonstrate the implementation of the predictive control algorithm for an initial condition ($C_I(0) = 0.11\ kmolm^{-3}$, $C_M(0) = 3.73\ kmolm^{-3}$, $T(0) = 334.92\ K$, $T_c(0) = 314.24\ K$) outside the set Ω^+. As can be seen from the solid lines in Figs.2.6–2.7 (which show the evolution of the state and input profiles), even though the initial condition is significantly outside the stability region estimate, the predictive controller is able to stabilize the closed–loop system. We next investigate the robustness of the predictive controller with respect to parametric uncertainty and disturbances from an initial condition $C_I(0) = 0.05\ kmolm^{-3}$, $C_M(0) = 2.45\ kmolm^{-3}$, $T(0) = 372.66\ K$, $T_c(0) = 332.05\ K$. Specifically, we consider errors in the values of the parameters A_p, hA and V_c of magnitude +1%, +2% and +10%, respectively as well as sinusoidal disturbances in the initiator flow rate F_i and the coolant inlet temperature T_{cf} of the form $+0.01F_{i,n}\sin(t/10)$ and $+0.01T_{cf,n}\sin(t/2)$ respectively, where the subscript n denotes the nominal steady–state values. These parametric errors and disturbances result in a change in the value of the nominal steady state. The predictive controller is however able to offset the effect of the parametric errors and disturbances demonstrating robust stabilization the closed–loop system (see dashed lines in Figs.2.6–2.7).

2.5 Conclusions

This chapter considered the problem of predictive control of nonlinear process systems subject to input constraints. A predictive controller for linear systems was first designed that achieves stability for every initial condition in the null controllable region without resorting to infinite horizons. For nonlinear process systems, predictive controllers were designed that expand on the set of initial conditions from where closed–loop stability is achievable. The proposed method was illustrated using a chemical reactor example and the robustness with respect to parametric uncertainty and disturbances demonstrated via application to a styrene polymerization process.

Table 2.1: Chemical reactor parameters and steady–state values.

V	$=$	0.1	m^3
R	$=$	8.314	$KJ/Kmol \cdot K$
C_{A0_s}	$=$	1.0	$Kmol/m^3$
T_{A0_s}	$=$	310.0	K
Q_s	$=$	0.0	KJ/min
ΔH	$=$	-4.78×10^4	$KJ/Kmol$
k_0	$=$	72×10^9	min^{-1}
E	$=$	8.314×10^4	$KJ/Kmol$
c_p	$=$	0.239	$KJ/Kg \cdot K$
ρ	$=$	1000.0	Kg/m^3
F	$=$	100×10^{-3}	m^3/min
T_{Rs}	$=$	395.33	K
C_{As}	$=$	0.57	$Kmol/m^3$

Table 2.2: Styrene polymerization parameter values and units.

F_i	=	3×10^{-4}	$m^3 s^{-1}$
F_m	=	10.5×10^{-4}	$m^3 s^{-1}$
F_s	=	12.75×10^{-4}	$m^3 s^{-1}$
F_t	=	26.25×10^{-4}	$m^3 s^{-1}$
F_c	=	13.1×10^{-4}	$m^3 s^{-1}$
$C_{If,n}$	=	0.5888	$kmolm^{-3}$
C_I	=	0.0480	$kmolm^{-3}$
$C_{Mf,n}$	=	9.975	$kmolm^{-3}$
C_M	=	2.3331	$kmolm^{-3}$
$T_{f,n}$	=	306.71	K
T	=	354.9205	K
$T_{cf,n}$	=	294.85	K
T_c	=	316.2429	K
A_d	=	5.95×10^{14}	s^{-1}
A_t	=	1.25×10^{10}	s^{-1}
A_p	=	1.06×10^{8}	$kmolm^{-3} s^{-1}$
E_d/R	=	14.897×10^{3}	K
E_t/R	=	8.43×10^{2}	K
E_p/R	=	3.557×10^{3}	K
f	=	0.6	
ΔH	=	-1.67×10^{4}	$kJkmol^{-1}$
ρc_p	=	360	$kJm^{-3}K^{-1}$
hA	=	700	$JK^{-1}s^{-1}$
$\rho_c c_{pc}$	=	966.3	$kJm^{-3}K^{-1}$
V_{pr}	=	3.0	m^3
V_c	=	3.312	m^3

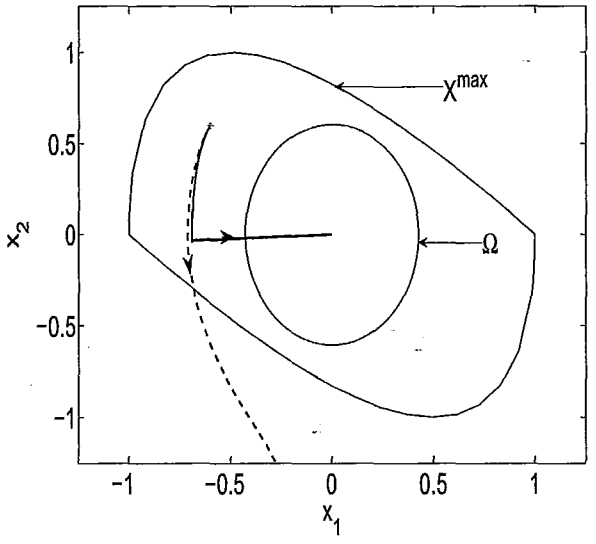

Figure 2.1: Evolution of the state trajectory for the linear system example under the predictive controller of Eqs.2.3–2.7 (dashed line) with a stability region Ω and under the proposed predictive controller (solid line) with a stability region X^{max}.

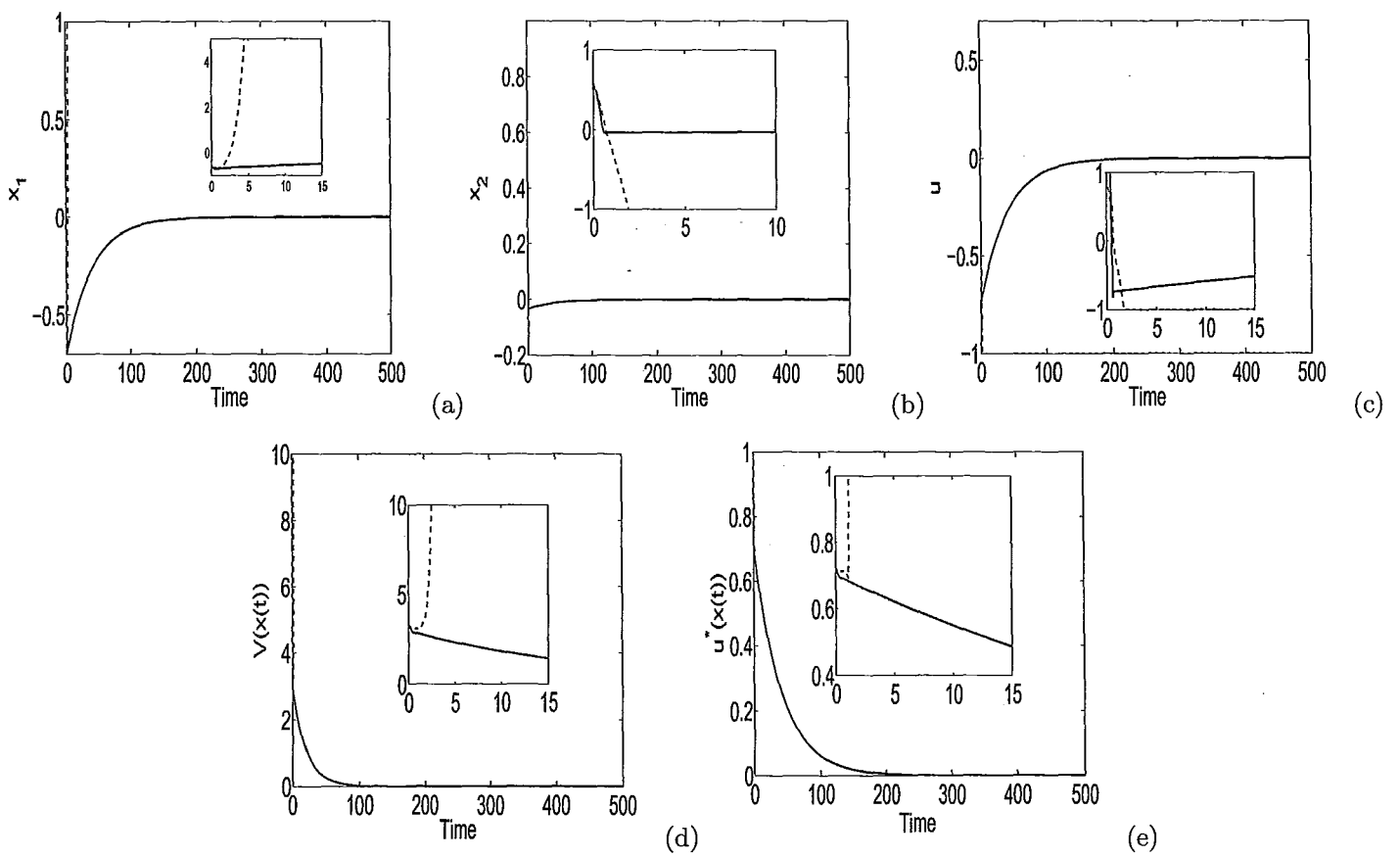

Figure 2.2: The state (a-b) and input profiles (c) and the evolution of the Lyapunov function (d) and $u^*(x(t))$ (e) for the linear system example under the predictive controller of Eqs.2.3–2.7 (dashed lines) and under the proposed predictive controller (solid lines). The insets show the initial evolution of the system.

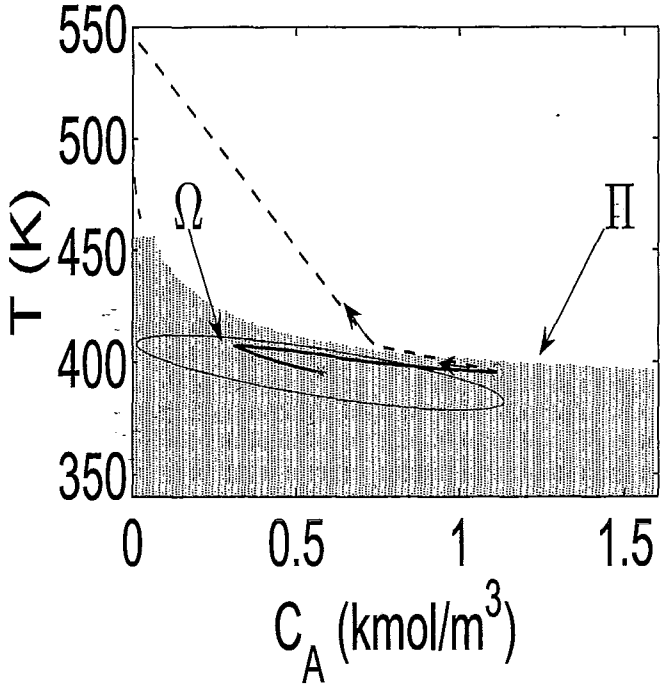

Figure 2.3: Evolution of the state trajectory for the chemical reactor example under the predictive controller of Eqs.2.3–2.7 (dashed line) with a stability region Ω and under the proposed predictive controller (solid line) enabling stabilization from initial conditions outside Ω.

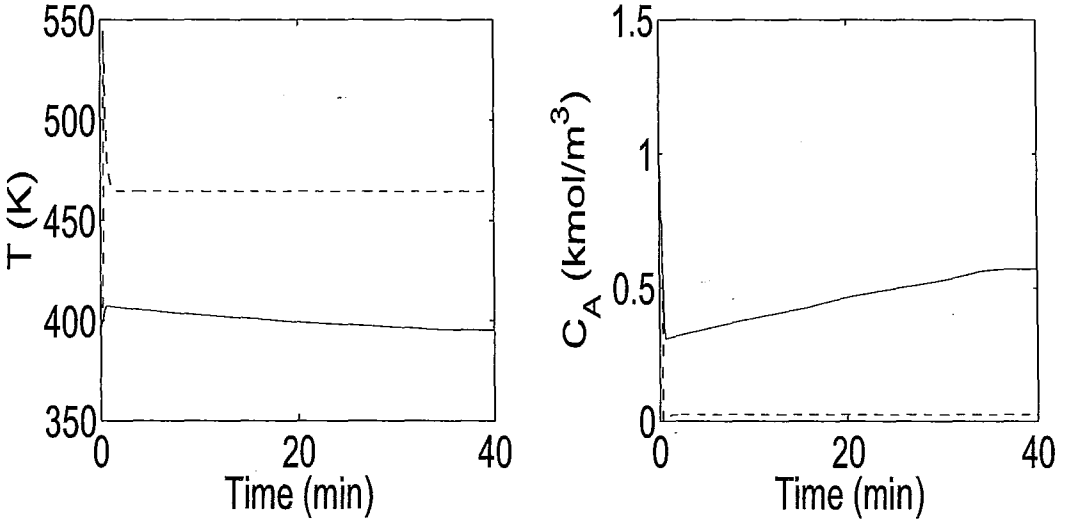

Figure 2.4: The state profiles for the chemical reactor example under the predictive controller of Eqs.2.3–2.7 (dashed lines) and under the proposed predictive controller (solid lines) from an initial condition outside Ω.

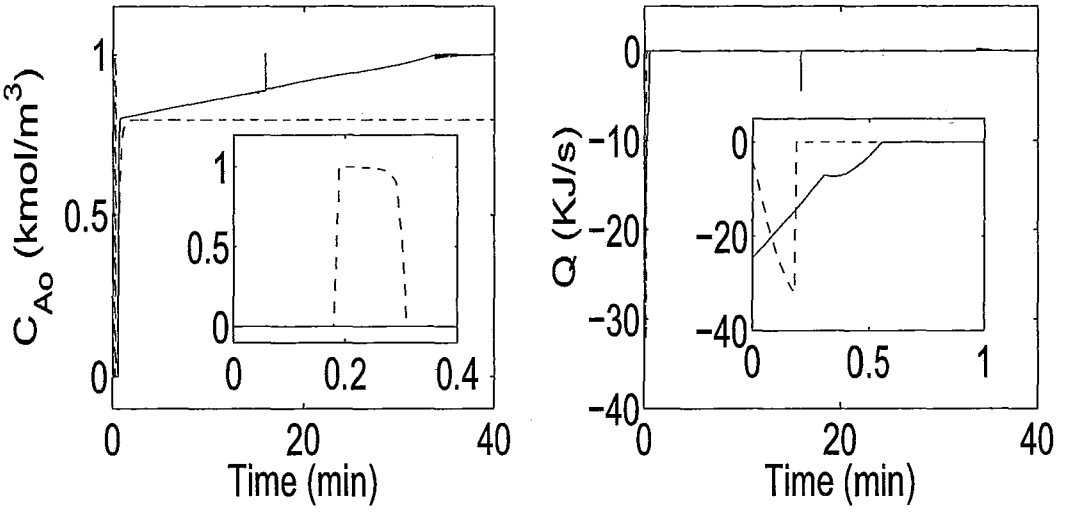

Figure 2.5: The input profiles for the chemical reactor example under the predictive controller of Eqs.2.3–2.7 (dashed lines) and under the proposed predictive controller (solid lines) from an initial condition outside Ω.

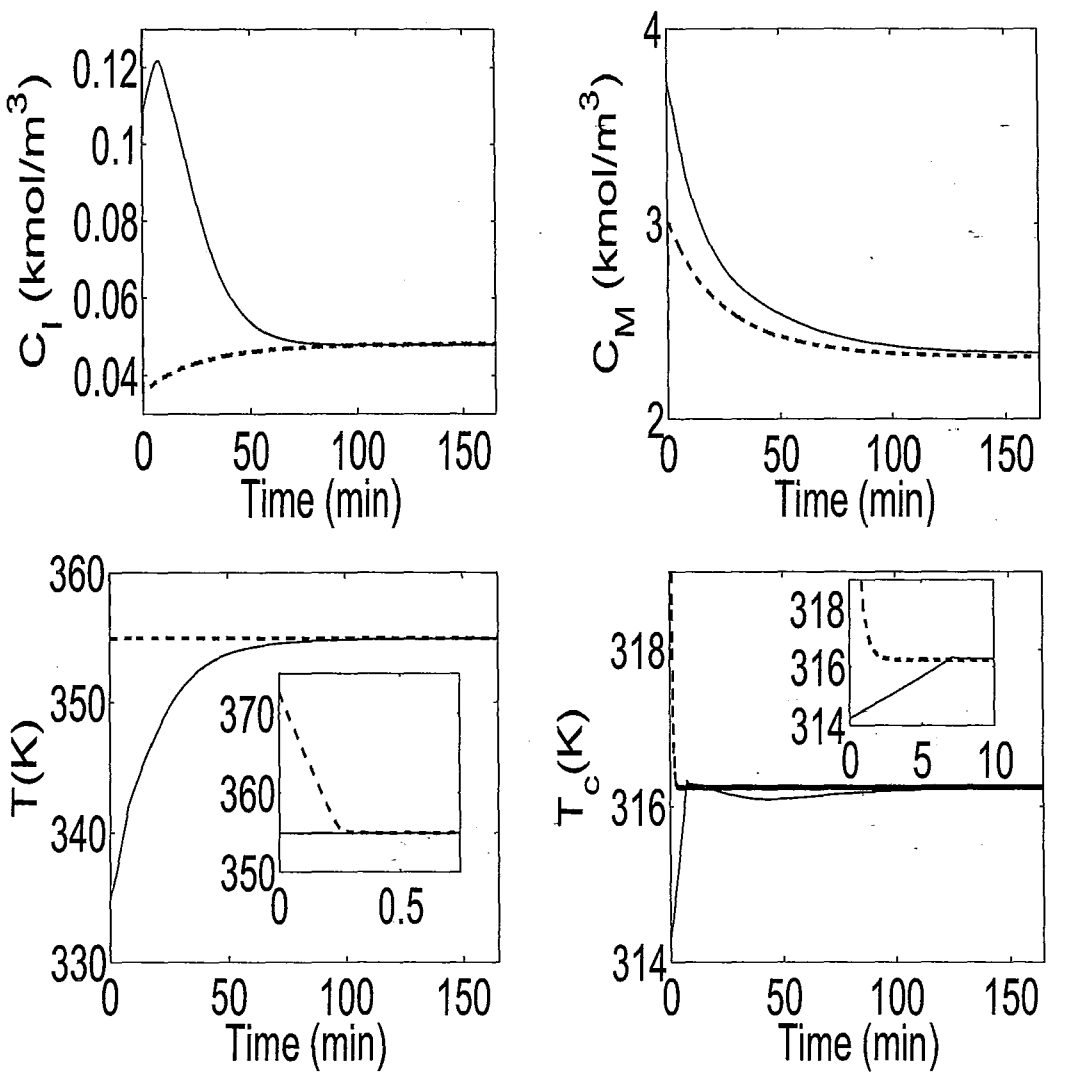

Figure 2.6: Evolution of the state profiles for the styrene polymerization process under the proposed predictive controller in the absence (solid lines) and presence of disturbances (dashed lines).

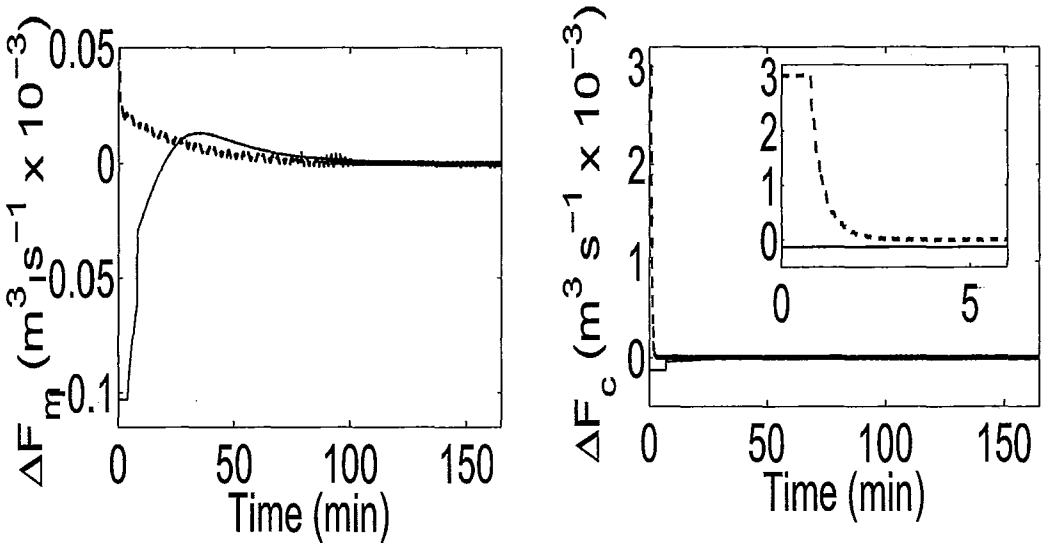

Figure 2.7: The input profiles showing the deviations from the nominal monomer and coolant flowrates for the styrene polymerization process under the proposed predictive controller in the absence (solid lines) and presence of disturbances (dashed lines).

Chapter 3

Safe-Parking of Nonlinear Process Systems: Handling Uncertainty and Unavailability of Measurements

3.1 Introduction

The operation and control of chemical processes is experiencing increased reliance on automation with the enhanced availability of sensors and actuators and communication infrastructure. The increased availability of information has opened up several opportunities in making better use of the available resources and coordinating safety measures across the plant. The resulting interdependence of processing units, both materially and in terms of information flow, has also placed more emphasis on the need to preserve safe plant operation to handle eventualities and contain the effects of faults to local processing units. Even under 'normal' operating conditions, chemical processes exhibit significant complexity (manifested as nonlinearities) and control designs have to account for operational issues

such as constraints, disturbances and availability of limited measurements. Safe and profitable operation of chemical processes, therefore, relies on the design and implementation of control algorithms that can handle process complexity as well as respond to, and minimize the negative effect of, eventualities.

The extensive economic, personnel and environmental damage caused by the faults (it is estimated that the U.S. petrochemical industry loses an estimated $20 billion per year due to faults; see e.g., [15] and the references therein) as well as the practical inevitability of fault occurrence has motivated several researchers to consider the problem of handling of faults. The first step in handling of faults is the ability to detect and isolate the faults. Statistical and pattern recognition techniques for data analysis and interpretation (e.g., [45; 72; 66; 65; 18; 2]) use historical plant-data to construct indicators that identify deviations from normal operation to detect faults. The problem of using fundamental process models for the purpose of detecting faults has been studied extensively in the context of linear systems (e.g., [53; 33; 34; 55]); and more recently, fundamental results in the context of nonlinear systems have been derived (e.g., [74; 20; 68]).

In this chapter, we focus on mechanisms that must be put in place to handle a fault after it has been detected and isolated. The existing results on fault handling have focussed on continued operation at the nominal operating point, under the assumption of sufficiency of the depleted control action to preserve nominal operation. Under this assumption, one approach dictates fault-accommodation via robust/reliable control designs (e.g., see [84]) that allow continued operation at the nominal equilibrium point via controller-retuning. To handle the situation when the fault causes such significant depletion of the control action that prevents the handling of fault via controller re-tuning, other approaches assume the existence of redundant control configurations to preserve closed–loop stability. In the choice of redundant control configuration, however, the presence of nonlinearity, input constraints and uncertainty, as well as the hybrid nature of the closed–loop process must be accounted for.

The development of the above-mentioned reconfiguration–based approaches has been fa-

cilitated by extensive research on control of nonlinear and switched systems (see, e.g., [48; 79; 41; 54; 22; 58; 59; 16]). These include Lyapunov-based nonlinear control designs (see, e.g., [48; 28] for a review, see [16]) 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, [54]) 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 [58; 59] that allow explicit characterization of the stability region, via mimicking the stability properties of Lyapunov-based bounded controllers, without assuming initial feasibility of the optimization problem. In chapter 2 of this thesis a model predictive controller design was presented which better utilizes the constraint handling capabilities of model predictive controllers and enhances the set of initial conditions from where stability is achieved. The work in chapter 2 (also appeared in [52]), however, does not explicitly consider uncertainty and assumes the availability of complete state information. One of the contributions of the work in this chapter is the generalization of the predictive controller of chapter 2 to explicitly consider uncertainty and availability of limited measurements for subsequent use within a fault-handling framework.

In [60; 56; 25; 30; 61] reconfiguration-based fault-tolerant control structures have been developed that guarantee preservation of closed–loop stability using redundant control configurations. 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 [60; 56; 25; 30; 61] assume the existence of a backup, redundant control configuration. The scenario where a fault results in temporary 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 onset of hazardous situations and process shutdown with substantially negative economic ramifications. Recently, in [36] a 'safe-parking' framework was developed that preserves process safety and enables smooth resumption of

nominal operation on fault repair via identifying appropriate 'safe-park' points where the process is stabilized during failure. The safe-parking framework in [36], assumes availability of the entire state information as well as precise process dynamics knowledge. Availability of limited measurements and the presence of disturbances and uncertainty, however, can destabilize even nominal operation and also invalidate the guarantees of safe-parking and resumption of smooth operation upon fault-repair.

Motivated by the above considerations, the work in this chapter considers the problem of handling faults in control of nonlinear process systems subject to input constraints, uncertainty and unavailability of measurements. A framework is developed to handle faults that preclude the possibility of continued operation at the nominal equilibrium point using robust or reconfiguration-based fault-tolerant control approaches. The key consideration is to operate the plant using the depleted control at an appropriate 'safe-park' point to prevent onset of hazardous situations as well as enable smooth resumption of nominal operation upon fault-repair. In determining the safe-park point, dynamic considerations (via stability regions) are incorporated over and above the steady state considerations (via determining existence of equilibrium points for acceptable values of the functioning actuators). The rest of the chapter is organized as follows: we first present, in Section 3.2.1, the class of processes considered, followed by a styrene polymerization process in Section 3.2.2 and formulate the safe-parking problem in Section 3.2.3. In Section 3.3.1 we extend the results in chapter 2 to develop a robust Lyapunov-based predictive controller that enhances the set of initial conditions from where stabilization is achieved subject to uncertainty and present a safe-parking design that addresses the presence of uncertainty in Section 3.3.2. The problem of availability of limited measurements is handled in the control design in Section 3.4.1 and incorporated in the safe-parking framework in Section 3.4.2. A chemical reactor example is used to illustrate the details of the safe-parking framework in Sections 3.3.3 and 3.4.3 while application to the styrene polymerization process is demonstrated in Section 3.5. Finally, in Section 3.6 we summarize our results.

3.2 Preliminaries

In this section, we describe the class of processes considered, followed by a motivating example of a polystyrene process and then a formalization of the control problem.

3.2.1 Process description

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

$$\begin{aligned} \dot{x}(t) &= f(x(t)) + G(x(t))u_\sigma(t) + W(x)\theta(t) \\ y(x(t)) &= h(x(t)); u_\sigma(\cdot) \in \mathbf{U}_\sigma,\ \theta \in \Theta \end{aligned} \tag{3.1}$$

where $x \in \mathbb{R}^n$ and $y \in \mathbb{R}^m$ denote the vector of state and measured output variables, $u_\sigma(t) \in \mathbb{R}^m$ denotes the vector of constrained manipulated inputs, taking values in a nonempty convex subset $\mathbf{U}_\sigma$ of $\mathbb{R}^m$, where $\mathbf{U}_\sigma = \{u \in \mathbb{R}^m : u_{min,\sigma} \leq u \leq u_{max,\sigma}\}$, where $u_{min,\sigma}, u_{max,\sigma} \in \mathbb{R}^m$ denote the constraints on the manipulated inputs, $\theta(t) = [\theta^1(t) \cdots \theta^q(t)]^T \in \Theta \subset \mathbb{R}^q$ where $\Theta = \{\theta \in \mathbb{R}^q : \theta_{min} \leq \theta \leq \theta_{max}\}$, where $\theta_{min}, \theta_{max} \in \mathbb{R}^q$ denote the bounds on the vector of uncertain (possibly time–varying) but bounded variables taking values in a nonempty compact convex subset of $\mathbb{R}^q$, $f(0) = 0$ and $\sigma \in \{1, 2\}$ is a discrete variable that indexes the fault-free ($\sigma = 1$) and faulty ($\sigma = 2$) operation. Without loss of generality, the equilibrium point $x = 0$, is assumed to be the point of nominal operation.

The vector function $f(x)$ and the matrices $W(x)$, $G(x) = [g^1(x) \cdots g^m(x)]$ where $g^i(x) \in \mathbb{R}^n$, $i = 1 \cdots m$ are assumed to be locally Lipschitz. We also assume the existence of a control Lyapunov function $V : \mathbb{R}^n \to \mathbb{R}$, which will be subsequently used within the control design. Throughout the chapter, we assume $L_f V$, $L_G V$, $L_W V$ are locally Lipschitz functions, where the notation $L_\chi h$ denotes the standard Lie derivative of a scalar function $h(\cdot)$ with respect to the vector function $\chi(\cdot)$. 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 $B \backslash A$, where A and B are sets,

refers to the relative complement, defined by $B \backslash A = \{x \in B : x \notin A\}$.

3.2.2 Motivating example

To motivate the safe-parking framework and to demonstrate an application of our results, we introduce in this section a polystyrene polymerization process. To this end, consider the following model for a polystyrene polymerization process given in [39] (also studied in, e.g., [69], [52] and [36], where it is used in the context of demonstrating the stability properties of a new predictive controller design and the safe-parking framework in the absence of uncertainty and availability of full state information)

$$\begin{aligned}
\dot{C}_I &= \frac{(F_i C_{If} - F_t C_I)}{V_{pr}} - k_d C_I \\
\dot{C_M} &= \frac{(F_m C_{Mf} - F_t C_M)}{V_{pr}} - k_p C_M C_P \\
\dot{T} &= \frac{F_t(T_f - T)}{V_{pr}} + \frac{(-\Delta H)}{\rho c_p} k_p C_M C_P - \frac{hA}{\rho c_p V}(T - T_c) \\
\dot{T_c} &= \frac{F_c(T_{cf} - T_c)}{V_c} + \frac{hA}{\rho_c c_{pc} V_c}(T - T_c) \\
C_P &= \left[\frac{2 f k_d C_I}{k_t}\right]^{\frac{1}{2}} \\
k_d &= A_d e^{\frac{-E_d}{RT}} \\
k_p &= A_p e^{\frac{-E_p}{RT}} \\
k_t &= A_t e^{\frac{-E_t}{RT}}
\end{aligned} \tag{3.2}$$

where C_I, C_{If}, C_M, C_{Mf}, refer to the concentrations of the initiator and monomer in the reactor and inlet stream, respectively, T and T_f refer to the reactor and inlet stream temperatures and T_{cf} and T_c refer to the coolant inlet and jacket temperatures, respectively. The manipulated inputs are the monomer and coolant flow rates, denoted by F_m and F_c, respectively. As is the practice with the operation of the polystyrene polymerization process [39], the solvent flow rate is also changed in proportion to the monomer flow rate. The values of the process parameters are given in Table 3.1. The control objective is to stabilize

the reactor at the equilibrium point ($C_I = 0.07\ kmol/m^3$, $C_M = 3.97\ kmol/m^3$, $T = 303.55\ K$, $T_c = 297.95\ K$), corresponding to the nominal values of the manipulated inputs of $F_c = 1.31\ L/s$ and $F_m = 1.05\ L/s$. The manipulated inputs are constrained as $0 \leq F_c \leq 31.31\ L/s$ and $0 \leq F_m \leq 31.05\ L/s$.

Consider the scenario where the valve manipulating the coolant flow rate fails and reverts to the fail-safe position (fully open). With the coolant flow rate set to the maximum, there simply does not exist an admissible value of the functioning manipulated input F_m, such that the nominal equilibrium point remains an equilibrium point for the process, precluding the possibility of continued operation at the nominal equilibrium point (regardless of the choice of the control law). The key problem is to determine how to operate the process under failure conditions to maintain process safety and, upon fault-repair, efficient resumption of nominal operation. We will demonstrate the application of the proposed safe-parking framework on the styrene polymerization process subject to uncertainty and limited availability of (noisy) measurements in Section 3.5, while illustrating the details of the proposed framework using a chemical reactor in Sections 3.3.3 and 3.4.3.

3.2.3 Problem definition

We consider faults in the control actuators under the assumption that upon failure, the actuator reverts to a fail-safe position. Examples of fail-safe positions include fully open for a valve regulating a coolant flow rate, fully closed for a valve regulating a steam flow etc. Specifically, we characterize the fault occurring without loss of generality, in the first control actuator at a time T^{fault}, subsequently rectified at a time T^{repair} (i.e., for $t \leq T^{fault}$ and $t > T^{repair}$, $\sigma(t) = 1$ and $\sigma(t) = 2$ for $T^{fault} < t \leq T^{repair}$), as $u_2^1(t) = u_{failed}^1$, with $u_{min,2}^1 \leq u_{failed}^1 \leq u_{max,2}^1$, where u^i denotes the ith component of a vector u, for all $T^{fault} < t \leq T^{repair}$, leaving only u_2^i, $i = 2 \ldots m$ 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 $X_c := \{x_c \in \mathbb{R}^n : f(x_c) + g^1(x_c)u_{failed}^1 + \sum_{i=2}^m g^i(x_c)u_2^i = 0,\ u_{min}^i \leq u_2^i \leq u_{max}^i, i = 2, \ldots, m\}$. The safe-

park candidates therefore represent possible equilibrium points (note that the subsequent results do not require the set of equilibrium points to be connected), corresponding to the failed actuator stuck at the fail-safe value, and acceptable values of the other manipulated inputs. Note that if $u^1_{failed} \neq 0$, 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. In other words, if one of the manipulated input fails and reverts to a fail-safe position, it may happen that no admissible combination of the functioning inputs exists for which the nominal equilibrium point continues to be an equilibrium point. Maintaining the functioning actuators at the nominal values may result in the onset of hazardous or undesirable process conditions or drive the process state to a point from where it may not be possible to resume nominal operation upon fault-repair. We define the safe-parking problem as the one of identifying safe-park points $x_s \in X_c$ that preserve process safety and allow smooth resumption of nominal operation upon fault-repair subject to uncertainty and availability of limited measurements.

3.3 Safe-parking of nonlinear process systems: handling uncertainty

The presence of uncertainty can invalidate the stability guarantees of the Lyapunov-based predictive controller developed in chapter 2, as well as the the safe-parking framework of [36]. To handle uncertainty, we first develop a robust predictive controller that provides an explicit characterization of the robust stability region (without assuming initial feasibility and without resorting to min-max computations), as well as enhances the set of initial conditions from where stabilization is achieved in Section 3.3.1 and then present a safe-parking algorithm handling uncertainty in Section 3.3.2.

3.3.1 Robust model predictive controller

In this section we present a robust predictive controller, for each mode of operation (and drop the subscript σ for ease of notation) that allows an explicit characterization of the feasibility and stability region and fully exploits the constraint handling capabilities of the predictive control approach. Using a control Lyapunov-function V, we define the set

$$\Pi = \{x \in \mathbb{R}^n : \sup_{\theta \in \Theta} \inf_{u \in \mathbf{U}} L_f V(x) + L_W V(x)\theta + L_G V(x)u + \rho V(x) \leq 0\} \tag{3.3}$$

where $L_G V = [L_{g^1} V \ \cdots \ L_{g^m} V]$ is a row vector (for a discussion on the definition of the set Π, see Remark 1). The $\sup_{\theta \in \Theta} \inf_{u \in \mathbf{U}}$ can be easily computed by determining the sign of the elements within the $L_W V$ and $L_G V$ terms. For instance, if $L_{W_i} V(x) \leq 0$, then the supremum is obtained for $\theta^i = \theta^i_{max}$, where $L_{W_i} V(x)$ and θ^i denote the ith elements of the vectors $L_W V(x)$ and θ respectively. Similarly, if $L_{G_i} V(x) \geq 0$, then the infimum is obtained for $u^i = u^i_{min}$, where $L_{G_i} V(x)$ and u^i denote the ith elements of the vectors $L_G V(x)$ and u respectively. For all values of the state in the set Π, therefore, there exists a value of the manipulated input that satisfies the constraints (note that the definition of the set Π does not depend on any specific control law, but only on the Lyapunov function, the process dynamics, input constraints and uncertainty) and also counters the effect of uncertainty on the Lyapunov function derivative. An estimate of the stability region can be constructed using a level set of V, i.e

$$\Omega := \{x \in \mathbb{R}^n : V(x) \leq c^{max}\} \tag{3.4}$$

where $c^{max} > 0$ is the largest number for which $\Omega \subseteq \Pi$. Consider now the receding horizon implementation of the control action computed by solving an optimization problem of the form:

$$u_{MPC}(x) := \arg min\{J(x, t, u(\cdot))|u(\cdot) \in S\} \tag{3.5}$$

$$s.t. \ \dot{x} = f(x) + G(x)u \tag{3.6}$$

$$L_G V(x(t))u(x(t)) \leq \sup_{\theta \in \Theta} -L_f V(x(t)) - L_W V(x(t))\theta - \rho V(x(t)) \tag{3.7}$$

$$x(\tau) \in \Pi \ \forall \ \tau \in [t, t + \Delta) \tag{3.8}$$

where ρ is a constant, $S = S(t,T)$ is the family of piecewise continuous functions (functions continuous from the right), with period Δ, mapping $[t, t+T]$ into $\mathbf{U}$. Eq.3.6 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

$$J(x,t,u(\cdot)) \;=\; \int_t^{t+T} \left[\|x^u(s;x,t)\|_Q^2 + \|u(s)\|_R^2\right] ds \tag{3.9}$$

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.3.6, due to control u, with initial state x at time t and T is the specified horizon. The minimizing control $u^0_{MPC}(\cdot) \in S$ is then applied to the plant over the interval $[t, t+\Delta)$ and the procedure is repeated indefinitely. Feasibility of the optimization problem and how it depends on Δ and the stability properties of the closed–loop system under the predictive controller are formalized in Theorem 3.1 below.

Theorem 3.1 : *Consider the constrained system of Eq.3.1 under the MPC law of Eqs.3.5–3.9. Then, given any positive real number d, 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.3.5-3.9 is guaranteed to be initially and successively feasible,* $x(t) \in \Omega \; \forall \; t \geq 0$ *and* $\limsup_{t\to\infty} \|x(t)\| \leq d$. *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* $\limsup_{t\to\infty} \|x(t)\| \leq d$.

Proof of Theorem 3.1: The proof of this theorem is divided in three parts. In the first part we show for all $x_0 \in \Omega$, the optimization problem of Eqs.3.5-3.9 is guaranteed to be initially feasible. We then show that there exists a Δ^* such that if $\Delta \in (0,\ \Delta^*]$ then Ω is invariant under receding horizon implementation of the predictive controller of Eqs.3.5-3.9 (implying that the optimization problem continues to be feasible) and that the state trajectories converge to the desired neighborhood of the origin. Finally, in part 3, we show that the state trajectories, once they reach the desired neighborhood of the origin, continue to stay in the neighborhood.

Part 1: Consider some $x_0 \in \Omega$ under receding horizon implementation of the predictive

controller of Eqs.3.5-3.9, with a prediction horizon $T = N\Delta$, where Δ is the hold time and $1 \leq N < \infty$ is the number of the prediction steps. We first analyze the constraint of Eq.3.7 for feasibility. Since $\Omega \subseteq \Pi$ and $x_0 \in \Omega$, this implies that there exists a $u \in S$ such that $L_G V(x)u(t) \leq \sup_{\theta \in \Theta} -L_f V(x) - L_W V(x)\theta(t) - \rho V(x)$. Therefore, for all $x(0) \in \Omega$, the solution comprising of u^* as the first element followed by $N-1$ zeros is a feasible solution to constraint of Eq.3.7.

Part 2: Having shown initial feasibility of the optimization problem in Part 1, we now show that the implementation of the control action computed by solving the optimization problem of Eqs.3.5-3.9 guarantees that for a given d, if we pick a sufficiently small Δ (i.e., there exists a Δ^* such that if $\Delta \in (0, \Delta^*])$ Ω is invariant under the predictive control algorithm of Eqs.3.5-3.9 (this would guarantee subsequent feasibility of the optimization problem due to part 1 above), and then that if the optimization problem continues to be feasible, then practical stability (convergence to a desired neighborhood of the origin) for the closed–loop system is achieved.

To this end, we first note that since $V(\cdot)$ is a continuous function of the state, one can find a finite, positive real number, δ', such that $V(x) \leq \delta'$ implies $\|x\| \leq d$. Now consider a "ring" close to the boundary of Ω, described by $\mathcal{M} := \{x \in \mathbb{R}^n : (c^{max} - \delta) \leq V(x) \leq c^{max}\}$, for a $0 \leq \delta < c^{max}$, with δ to be determined later. The initial feasibility of the constraint of Eq.3.7 implies that for all $x(0) \in \Omega$ and $\|\theta(t)\| \leq \theta_b$

$$\begin{aligned} \dot{V}(x) &= L_f V + L_G V u + L_W V \theta(t) \\ &\leq -\rho V(x) \end{aligned} \tag{3.10}$$

Furthermore, if the control action is held constant until a time Δ^{**}, where Δ^{**} is a positive real number $(u(t) = u(x_0) := u_0 \; \forall \, t \in [0, \Delta^{**}])$ then, $\forall \, t \in [0, \Delta^{**}]$,

$$\begin{aligned} \dot{V}(x(t)) &= L_f V(x(t)) + L_G V(x(t))u_0 + L_W V(x(t))\theta(t) \\ &= L_f V(x_0) + L_G V(x_0)u_0 + L_W V(x_0)\theta(0) + (L_f V(x(t)) - L_f V(x_0)) \\ &\quad + (L_G V(x(t))u_0 - L_G V(x_0)u_0) + L_W V(x(t))\theta(t) - L_W V(x_0)\theta(0) \end{aligned} \tag{3.11}$$

Since $x_0 \in \mathcal{M} \subseteq \Omega$, and $\theta \in \Theta$, $L_f V(x_0) + L_G V(x_0)u_0 + L_W V(x_0)\theta(0) \leq -\rho V(x_0)$. By definition, for all $x_0 \in \mathcal{M}$, $V(x_0) \geq c^{max} - \delta$, therefore $L_f V(x_0) + L_G V(x_0)u_0 +$

$L_W V(x_0)\theta(0) \leq -\rho(c^{max}-\delta)$. Since the function $f(\cdot)$ and the elements of the matrices $G(\cdot)$, $W(\cdot)$ are continuous, $\|u(t)\| \leq u^{max}$, $\|\theta(t)\| \leq \theta^{max}$ and $\mathcal{M}$ is bounded, then one can find, for all $x_0 \in \mathcal{M}$ and a fixed Δ^{**}, a positive real number K^1, such that $\|x(t) - x_0\| \leq K^1\Delta^{**}$ for all $t \leq \Delta^{**}$.

Since the functions $L_f V(\cdot)$, $L_G V(\cdot)$, $L_W V(\cdot)$ are locally Lipschitz, then given that $\|x(t) - x_0\| \leq K^1\Delta^{**}$, $x_0 \in \Omega$ and $\|\theta(t)\| \leq \theta^{max}$, we have that one can find positive real numbers K^2, K^3 and K^4 such that $\|L_f V(x(t)) - L_f V(x_0)\| \leq K^3K^1\Delta^{**}$, $\|L_G V(x(t))u_0 - L_G V(x_0)u_0\| \leq K^2K^1\Delta^{**}$ and $\|L_W V(x(t))\theta(t) - L_W V(x_0)\theta(0)\| \leq K^4K^1\Delta^{**}$. Using these inequalities in Eq.3.11, we get

$$\dot{V}(x(t)) \leq -\rho(c^{max} - \delta) + (K^1K^2 + K^1K^3 + K^1K^4)\Delta^{**} \tag{3.12}$$

For a choice of $\Delta^{**} < \dfrac{\rho(c^{max} - \delta) - \epsilon}{(K^1K^2 + K^1K^3 + K^1K^4)}$ where ϵ is a positive real number such that

$$\epsilon < \rho(c^{max} - \delta) \tag{3.13}$$

we get that $\dot{V}(x(t)) \leq -\epsilon < 0$ for all $t \leq \Delta^{**}$. This implies that, given δ', if we pick δ such that $c^{max} - \delta < \delta'$ and find a corresponding value of Δ^{**} then if the control action is computed for any $x \in \mathcal{M}$, and the 'hold' time is less than Δ^{**}, we get that $\dot{V}$ remains negative during this time, and therefore the state of the closed–loop system cannot escape Ω (since Ω is a level set of V). This in turn implies successive feasibility of the optimization problem for all initial conditions in $\mathcal{M}$, and that for any initial condition, x_0, such that $\delta < V(x_0) \leq c^{max}$ we have that $V(x(t + \Delta)) < V(x(t))$. All trajectories originating in Ω, therefore converge to the set defined by $\Omega^f := \{x \in \mathbb{R}^n : V(x) \leq c^{max} - \delta\}$.

Part 3: We now show the existence of Δ' such that for all $x_0 \in \Omega^f := \{x \in \mathbb{R}^n : V(x_0) \leq c^{max} - \delta\}$, we have that $x(\Delta) \in \Omega^u := \{x_0 \in \mathbb{R}^n : V(x_0) \leq \delta'\}$, where $\delta' < c^{max}$, for any $\Delta \in (0, \Delta']$.

Consider Δ' such that

$$\delta' = \max_{V(x_0) \leq c^{max} - \delta,\ u \in \mathcal{U},\ \theta \in \Theta\ t \in [0, \Delta']} V(x(t)) \tag{3.14}$$

Since V is a continuous function of x, and x evolves continuously in time, then for any value of $\delta < c^{max}$, one can choose a sufficiently small Δ' such that Eq.3.14 holds. Let $\Delta^* = \min\{\Delta^{**}, \Delta'\}$. We now show that for all $x_0 \in \Omega^u$ and $\Delta \in (0, \Delta^*]$, $x(t) \in \Omega^u$ for all $t \geq 0$.

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

In summary, we showed 1) that for all $x(0) \in \Omega$, the optimization problem is guaranteed to be feasible, 2) the optimization problem continues to be feasible and $x(t) \in \Omega \; \forall \; t \geq 0$, all state trajectories originating in Ω converge to Ω^u, and 3) that all state trajectories originating in Ω^u stay in Ω^u, i.e., $x(t) \in \Omega \; \forall \; t \; \geq \; 0$ and $\limsup_{t \to \infty} \|x(t)\| \leq d$.

We next consider initial conditions such that $x_0 \in \Pi \backslash \Omega$. The initial and successive feasibility of the optimization problem ensures that $V(x(t+\Delta)) < V(x(t))$. All trajectories originating in Π, therefore converge to the set Ω. Once the state trajectory enters Ω, $x(t) \in \Omega \; \forall \; t \; \geq \; 0$ and $\limsup_{t \to \infty} \|x(t)\| \leq d$ can be showed as before. This completes the proof of Theorem 3.1. □

Remark 3.1: The proposed predictive controller ensures robust stability by computing the control action such that its effect on the evolution of the Lyapunov-function is sufficiently negative to counter the worst case effect of the disturbances on the Lyapunov function derivative. Feasibility of this constraint is guaranteed by explicitly characterizing the set Π for which an acceptable value of the manipulated input exists that can counter the effect of the state dynamics and uncertainty on the Lyapunov-function derivative. The term $\rho V(x)$ appears in the constraint of Eq.3.7 to provide "robustness" against the fact that the control action is computed for a certain state, but held for a time Δ during which time the process moves away from the state for which the control action was computed.

Theorem 3.1 establishes the existence of a robustness margin that allows practical stability

in the presence of disturbances and compute and hold control action. Preparatory to our results on the output feedback controller in section 3.4.1, we present a corollary that establishes the existence of an equivalent 'bound' on the error in the state variable measurements that the controller can tolerate, in the absence of uncertainty. The proof of the corollary follows along similar lines of Theorem 3.1 and is omitted for brevity.

Corollary 3.1 : *Consider the constrained system of Eq.3.1 with* $\theta(t) = 0$ *under the MPC law* $u_{MPC}(x + e)$ *designed using* $|\theta_{max}|, |\theta_{min}| > 0$. *There exists a positive real number* e_m *such that if* $|e| \leq e_m$ *and* $x_0 \in \Omega$, *then the optimization problem of Eqs.3.5-3.9 is guaranteed to be initially and successively feasible,* $x(t) \in \Omega \; \forall \; t \geq 0$ *and* $\limsup_{t \to \infty} \|x(t)\| \leq d$. *Furthermore, if* $x_0 \in \Pi \backslash \Omega$, *and if the optimization problem is successively feasible, then* $x(t) \in \Pi \; \forall \; t \geq 0$ *and* $\limsup_{t \to \infty} \|x(t)\| \leq d$.

Remark 3.2: The above corollary establishes the existence, for a given bound on the disturbances, of an equivalent robustness margin with respect to error in the value of the state variable measurements. Note that such a robustness margin with respect to errors in the state measurements can be incorporated in the controller over and above the robustness with respect to disturbances. For the sake of simplicity, in this chapter the 'equivalent' robustness with respect to measurement errors (in the absence of uncertainty) is analyzed. This 'equivalent' robustness is then subsequently used within the output feedback predictive controller in Section 3.4.1.

Remark 3.3: Note that the proposed robust predictive controller is different from existing robust MPC designs in that it does not use a min-max formulation (but guarantees stability for the nonlinear uncertain system) and also allows explicit characterization of the set of initial conditions for which the optimization problem is guaranteed (not assumed) to be feasible. The proposed robust predictive controller also differs from recently proposed Lyapunov-based predictive control designs. Specifically, the robust predictive control design in [56] uses an auxiliary control law in formulating the robust stability constraint and the stability region of the robust predictive controller of [56] is limited to the (possibly conservative) stability region estimate of the auxiliary control law. The Lyapunov-based

controller proposed in chapter 2 enhances the set of initial conditions from where closed–loop stability is achieved compared to Lyapunov-based bounded control designs. However, the predictive control design of chapter 2 does not explicitly account for the presence of disturbances and uncertainties. In contrast, the proposed robust predictive controller not only enhances the set of initial conditions from where stability is achieved, but also explicitly accounts for the presence of uncertainty in the control design.

Remark 3.4: Note that the estimates of the stability region are influenced by the choice of the control Lyuapunov function. Furthermore, referring to the choice of the CLF (and this holds for other Lyapunov-based control laws as well), it is important to note that a general procedure to construct CLFs for nonlinear process systems of the form Eq.3.6 is currently not available. Yet, for several classes of nonlinear systems that commonly arise in the modeling of engineering applications [22], it is possible to use a suitable approximation [22], or exploit system structure. One approach commonly used to construct (local) quadratic CLFs is by using the linearized system matrices to compute the solution of a Ricatti inequality. The stability properties of the nonlinear system can then be analyzed using the quadratic CLF. While not done in the present chapter, the entries in the matrix P can be further refined to mitigate possible conservatism in the stability region estimates, for instance, by formulating an optimization problem to determine (if possible) a Lyapunov function whose derivative can be made negative definite over a desired neighborhood of the origin.

3.3.2 Robust safe-parking of nonlinear process systems

The presence of uncertainty and constraints on the manipulated inputs need to be accounted for to ensure that upon failure, the process does not transit to a hazardous operating point, and this can be achieved via requiring 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 3.2 below. To this end, consider the system of Eq.3.1 for which the first control actuator fails at a time T^{fault} and is reactivated at time T^{repair}, and for which the robust stability region under nominal operation, denoted by Ω_n, has been characterized using the predictive controller formulation of Eqs.3.5–3.9. 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.3.5–3.9, and u_{2,x_c} as the control law designed to stabilize at the candidate safe-park (using the depleted control action) with u_{1,x_n} being the nominal control law (using all the control actuators).

Theorem 3.2 : *Consider the constrained system of Eq.3.1 under the MPC law of Eqs.3.5–3.9. If* $x(0) \in \Omega_n$, $x(T^{fault}) \in \Omega_c$ *and* $\Omega_c \subset \Omega_n$, *then the switching rule*

$$u(t) = \left\{ \begin{array}{lll} u_{1,n} & , & 0 \leq t < T^{fault} \\ u_{2,x_c} & , & T^{fault} \leq t < T^{repair} \\ u_{1,n} & , & T^{repair} \leq t \end{array} \right\} \tag{3.15}$$

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

Proof of Theorem 3.2: We consider the two possible cases; first if no fault occurs ($T^{fault} = T^{repair} = \infty$), and second if a fault occurs at a time $T^{fault} < \infty$ and is recovered at a time $T^{fault} \leq T^{repair} < \infty$.

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 3.1 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^{repair}. Since $x(T^{fault}) \in \Omega_c \subset \Omega_n$, we have that $x(t) \in \Omega_n \; \forall \; T^{fault} \leq t \leq T^{repair}$. At a time T^{repair}, we therefore also have that $x(T^{repair}) \in \Omega_n$. Subsequently, as with case 1, the nominal control configuration is implemented for all time thereafter, we have that $x(t) \in \Omega_n \; \forall \; t \geq T^{repair}$. 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 3.2. □

Remark 3.5: Note that the stability regions of candidate safe-parking points can be computed 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 (as is done for the nominal equilibrium point). Theorem 3.2 presents the conditions that must be met for a safe-park candidate to be chosen as the safe-park point. By requiring that the stability (and invariant) region of the candidate safe-park point be such that the process state at the time of the failure resides in the stability region for the safe-park point, it is ensured that the process can be driven to the point of safe-park with the depleted control action available. On the other hand, by requiring that the stability (and invariant) region for a safe-park point be completely contained in the stability region under nominal operation, it is ensured that the state trajectory always stays within the stability region under nominal operation, thereby enabling smooth resumption of nominal operation. Note that the second 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 under nominal operation, and it may happen that at the time of fault-repair, the closed–loop state trajectory does not reside in the stability region under nominal operation. However, to preserve closed–loop stability upon fault-repair, 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 3.6: The necessity of the requirements of Theorem 3.2 can be understood in the context of preventing onset of hazardous situations as well as enabling smooth resumption of nominal operation. Note that in the presence of an actuator failure, if the control law still tries to utilize the available control actuators to try to drive the process state to the nominal operating point, the active actuators may saturate and end up driving the process state to a hazardous operating point, or to a point from where nominal operation cannot be resumed upon fault-repair. On the other hand, if continued operation at the nominal operating point was possible either via the depleted control configuration or via control loop reconfiguration,

then reconfiguration-based fault-tolerant control approaches (e.g., see [56]) could be utilized to preserve closed–loop stability. However, Theorem 3.2 addresses the problem where a fault occurs that precludes operation at nominal operating point, and provides an appropriately characterized safe-park point where the process can be temporarily 'parked' until nominal operation can be resumed.

Remark 3.7: The assumption that the actuators revert to the fail-safe position upon failure reflects common practice wherein actuators have a built-in fail-safe position that they revert to upon failure. The fail-safe positions are typically determined to minimize possibilities of excursions to dangerous conditions such as high temperatures and pressures (setting a coolant valve to fail to a fully open position, while setting a steam valve to fail to a shut position). This assumption 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 $x(T^{fault}) \in \Omega_{x_s}$ has to be verified online, upon fault-occurrence, and can be done via simply evaluating the Lyapunov function). Note also 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 repair times, and only provides appropriate switching logic that is executed when, and if, a fault takes place and is subsequently rectified. We also note that the switch to the alternate control law involves the remaining (functioning) actuators, and does not involve invoking a backup actuator configuration (that could involve hardware delays). Delays in the present framework could arise due to the fault-detection and isolation time, and the proposed framework has the appropriate tools (via stability regions) to allow for the incorporation of such delays. In particular, the proposed strategy can be modified to incorporate a delay term such that the safe-park point is chosen based on the state position after the fault has been detected and isolated. Explicit incorporation of the fault-detection and isolation mechanism and the associated delays, however, remains outside the scope of the present work.

3.3.3 Illustrative simulation example: handling uncertainty

We illustrate in this section the proposed safe-park framework in the presence of uncertainty via a continuous stirred tank reactor (CSTR). To this end, 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:

$$\begin{aligned} \dot{C_A} &= \frac{F}{V}(C_{A,in} - C_A) - k_0 e^{\frac{-E}{RT_R}} C_A \\ \dot{C_B} &= \frac{F}{V}(C_{B,in} - C_B) + k_0 e^{\frac{-E}{RT_R}} C_A \\ \dot{T_R} &= \frac{F}{V}(T_{in} - T_R) + \frac{(-\Delta H)}{\rho_f c_p} k_0 e^{\frac{-E}{RT_R}} C_A + \frac{Q}{\rho_f c_p V} \end{aligned} \tag{3.16}$$

where C_A, C_B denotes the concentration of the species A, and B, respectively, 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_f are the heat capacity and fluid density in the reactor. The values of all process parameters can be found in Table 3.2. The control objective is to stabilize the reactor at the unstable equilibrium point $(C_A^s,\ T_R^s) = (0.45\ Kmol/m^3, 393\ K)$ in the presence of uncertainty. Specifically, we consider an error in the parameter ΔH of magnitude $+1\%$, and a sinusoidal disturbance in the inlet temperature T_{in} of the form $+0.05T_{in_s}\sin(t/0.02)$. We also consider random disturbances in F, $C_{A,in}$, and Q of the form $0.01\nu(t)F$, $0.01\nu(t)C_{A,in_s}$, and $0.05\nu(t)Q_s$ respectively. The variable $\nu(t)$ is an uniformly distributed random variable for each instance in time t which takes values in the interval $[0, 1]$ and is generated using MATLAB's pseudo random number generator function RAND. Manipulated variables are the rate of heat input/removal, Q, and change in inlet concentration of species A, $\Delta C_{A,in} = C_{A,in} - C_{A,in_s}$, with constraints: $|Q| \leq 32\ KJ/s$ and $0 \leq C_{A,in} \leq 2\ Kmol/m^3$. 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 $C_{A,in} = 0.73\ Kmol/m^3$ and $Q = 10\ KJ/s$.

For stabilizing the process at the nominal equilibrium point, the Lyapunov based MPC of Section 3.3.1 is designed using a quadratic Lyapunov function of the form $V = x^T P x$ with $P_N = \begin{bmatrix} 4.32 & 0 \\ 0 & 0.004 \end{bmatrix}$. The stability region is estimated and denoted by Ω in Fig.3.1. 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 $Q_1 = 0$). The nominal operating point corresponds to $Q_s = 10\ KJ/s$, and no value of the functioning manipulated inputs $-32\ KJ/s \leq Q_2 < 0\ KJ/s$ and $0 \leq C_{A,in} \leq 2\ Kmol/m^3$ exists such that the nominal equilibrium point continues to be an equilibrium point of the process subject to the fault. For $Q_2 = -30.72\ KJ/s$, $C_{A,in} = 1.86\ Kmol/m^3$ and $Q_2 = -4.57\ KJ/s$, $C_{A,in} = 1.26\ Kmol/m^3$, the corresponding equilibrium points are $S_1 = (1.05\ Kmol/m^3,\ 396\ K)$ and $S_2 = (0.8\ Kmol/m^3,\ 391.5\ K)$, which we denote as safe-park candidates. For each of these safe-park candidates, we also design Lyapunov based MPC of Section 3.3.1 using $P_{S_1} = \begin{bmatrix} 17.60 & 0 \\ 0 & 0.083 \end{bmatrix}$ for S_1 and $P_{S_2} = \begin{bmatrix} 9.30 & 0 \\ 0 & 0.027 \end{bmatrix}$ for S_2. The matrices in the objective function (Eq. 3.9), are chosen as $Q_w = \begin{bmatrix} 10^5 & 0 \\ 0 & 10^5 \end{bmatrix}$ and $R_w = \begin{bmatrix} 10^{-2} & 0 \\ 0 & 10^{-2} \end{bmatrix}$. Prediction and control horizons of 0.01 *min* are used in implementing the predictive controller.

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. At $t = 0.5\ min$, when the process state is at $F = (1\ Kmol/m^3,\ 393.76\ K)$, 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 $t = 1.7\ min$, the fault is rectified, however, we see that even after fault-repair, nominal operation cannot be resumed (see dashed lines in Fig.3.1). 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-repair (see solid lines in Fig.3.1). The

state and input profiles are shown in Fig.3.2. In summary, the simulation scenario illustrates the necessity to account for the presence of input constraints and uncertainty (characterized via the stability region) in the choice of the safe-park point.

3.4 Safe-parking of nonlinear process systems: handling availability of limited measurements

In the previous section, a robust safe-parking methodology was presented under the assumption of availability of the full state for feedback. In practice, the entire state information may often not be available and necessitates estimation of the process state via an appropriate state observer. We first develop in Section 3.4.1 a predictive controller formulation that provides guaranteed stability from an explicitly characterized set of initial conditions under availability of limited measurements. A safe-parking algorithm that accounts for the estimation errors associated with the state observer is subsequently presented in Section 3.4.2.

3.4.1 Output-feedback Lyapunov-based predictive controller

To allow for the output-feedback controller design, we impose the following assumption on the process of Eq.3.1.

Assumption 1. There exist a set of integers $(r_1, r_2, \ldots, r_m)$ *and coordinate transformations* $(\xi^{(i)} = T^{(i)}(x))$ *such that the representation of the system of Eq.3.1, in the* $\xi^{(i)}$ *coordinates takes the form*

$$\begin{aligned} \dot{\xi}_1^{(i)} &= \xi_2^{(i)} \\ &\vdots \\ \dot{\xi}_{r_i-1}^{(i)} &= \xi_{r_i}^{(i)} \\ \dot{\xi}_{r_i}^{(i)} &= L_f^{r_i} h_i(x) + \sum_{j=1}^{m} L_{g_j} L_f^{r_i-1} h_i(x) u_j \end{aligned} \tag{3.17}$$

where $L_{g_i} L_{f_i}^{n-1} h_{m_i}(x) \neq 0$ *for all* $x \in \mathbb{R}^n$. *Also,* $\xi^{(i)} \longrightarrow 0$ *if and only if* $x \longrightarrow 0$. Prepara-

tory to the presentation of the output feedback model predictive controller, we present an assumption below that formally characterizes the 'speed of escape' of the system states, i.e., establishes a time for which the process states will continue to reside in Ω given that the initial conditions are within a given subset of Ω.

Assumption 2. Consider the nonlinear system of Eq.3.1 with $u \in \mathbf{U}$. Then, given any positive real numbers $\delta > \delta_b$, there exists some time $T_b > 0$, such that if $V(x(0)) \leq \delta_b$, then $V(x(t)) \leq \delta \; \forall \; t \leq T_b$.

We now present the output feedback predictive controller (for a similar result in the context of sensor data losses, see [62]). To this end, consider again the nonlinear system of Eq.3.1, for which the parameter e_m (allowable error in the state values used in computing the control action) has been characterized (using Corollary 1), and for a given subset Ω_b (the desired output feedback stability region; characterized by δ_b), the time T_b (defined in Assumption 2) has also been computed.

Theorem 3.3 : *Consider the nonlinear system of Eq.3.1, under the output feedback MPC law of Eqs.3.5–3.9:*

$$\begin{aligned} \dot{\tilde{y}}^{(i)} &= \begin{bmatrix} -L_i a_1^{(i)} & 1 & 0 & \cdots & 0 \\ -L_i^2 a_2^{(i)} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -L_i^n a_r^{(i)} & 0 & 0 & \cdots & 0 \end{bmatrix} \tilde{y}_i + \begin{bmatrix} L_i a_1^{(i)} \\ L_i^2 a_2^{(i)} \\ \vdots \\ L_i^n a_n^{(i)} \end{bmatrix} y_m \\ u &= u_{mpc}(\hat{x}) \end{aligned} \tag{3.18}$$

where the parameters, $a_1^{(i)}, \cdots, a_n^{(i)}$ are chosen such that the polynomial $s^n + a_1^{(i)} s^{n-1} + a_2^{(i)} s^{n-2} + \cdots + a_n^{(i)} = 0$ is Hurwitz, $\hat{x} = [T_1^{-1}(\tilde{y}_1), \ldots, T_m^{-1}(\tilde{y}_m)]$, and let $\epsilon = max\{1/L_i\}$. Then, there exists positive real number ϵ^* such that if $\epsilon \in (0, \epsilon^*]$, $x(0) \in \Omega_b$ and $\hat{x}(0) \in \Omega_b$, then $x(t) \in \Omega \; \forall \; t \geq 0$ and $\limsup_{t \to \infty} \|x(t)\| \leq d$. Furthermore, for a choice of $\epsilon \in (0, \epsilon^*]$, $\|x(t) - \hat{x}(t)\| \leq e_m$ for all $t \geq T^b$.

Proof of Theorem 3.3: The proof of this theorem consists of two parts. In the first part, we use a singular perturbation formulation to represent the closed-loop system, with

the resulting fast subsystem being globally exponentially stable, and use this, together with Assumption 2 to show that for any $\hat{x}(0)$ and $x(0) \in \Omega_b$, there exists $\varepsilon^* > 0$ such that, for every $0 < \varepsilon < \varepsilon^*$, the state trajectory remains in the set Ω till the time that the state estimation error falls below a given value e_m. Then in the second part, we show practical stability of the closed–loop system using Corollary 1.

Part 1: Defining the auxiliary error variables $\hat{e}_j = L_i^{r_i-j}(y_i - \tilde{y}_j^{(i)})$, $j = 1, \ldots, r_i$, the vectors $e_0^{(i)} = [\hat{e}_1^i \hat{e}_2^{(i)}, \ldots, \hat{e}_{r_i}^{(i)}]^T$, $e_0 = [{e_o^{(1)}}^T, {e_o^{(2)}}^T, \ldots, {e_o^{(m)}}^T]$ the parameters $\varepsilon_i = 1/L_i$, the matrices $\tilde{A}_i$ and the vector $\tilde{b}_i$:

$$\tilde{A}_i = \begin{bmatrix} -a_1^{(i)} & 1 & 0 & \cdots & 0 \\ -a_2^{(i)} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_{r-1}^{(i)} & 0 & 0 & \ldots & 1 \\ -a_r^{(i)} & 0 & 0 & \cdots & 0 \end{bmatrix}, \tilde{b} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}, \tag{3.19}$$

the system of Eq.3.6 under the controller of Eq.3.18 takes the following form:

$$\varepsilon_i \dot{e}_o^{(i)} = \tilde{A}_i e_o^{(i)} + \varepsilon_i b \Psi(x, \hat{x}), i = 1, \ldots, m \tag{3.20}$$

$$\dot{x} = f(x) + g(x)u(\hat{x}) \tag{3.21}$$

where $\Psi(x, \hat{x})$ is a Lipschitiz function of its argument, with Lipschitz constant, κ, such that $\kappa \ll 1/\varepsilon_i$. Owing to the presence of the small parameter ε_i that multiplies the time derivative $\dot{e}_o^{(i)}$, the system of Eq.3.21 can be analyzed as a two-time-scale system. Defining $\bar{\varepsilon} = max\{\varepsilon_i\}$, multiplying each $e_0^{(i)}$ subsystem by $\bar{\varepsilon}/\varepsilon$ and introducing the fast time-scale $\tau = t/\bar{\varepsilon}$, and setting $\bar{\varepsilon}$=0, the closed-loop fast subsystem takes the form:

$$\frac{de_o^{(i)}}{d\tau} = \tilde{A}_i e_o \tag{3.22}$$

where each $\tilde{A}_i$ is Hurwitz. Establishing that the fast system is globally exponentially stable implies that for a given subset Ω_b, having computed T_b according to Assumption 2 (note that the state trajectory stays bounded for $t \leq T_b$) and also a positive real number e_m (defined in Corollary 1), there exists an ε^* such that if $\varepsilon \leq \varepsilon^*$, $|x(T_b) - \hat{x}(T_b)| \leq e_m$.

Part 2: Having established the convergence of the state estimates to a value less than e_m, by a time T_b, the results of Corollary 2 can be invoked to prove practical stability of the closed–loop system. This concludes the proof of Theorem 3.3. □

Remark 3.8: The output feedback controller in Eq.3.18 consists of a high-gain observer which provides estimates of the derivatives of the measured output y_m up to order $n-1$, denoted by $\tilde{y}_0, \tilde{y}_1, \ldots, \tilde{y}_{n-1}$, and thus estimates of variables $\xi_i^{(1)}, \ldots, \xi_i^{(n)}$ (see [43] for another example of an observer design for nonlinear systems). Note that the peaking phenomenon associated with the high-gain observer is naturally eliminated due to the presence of constraints on the manipulated input. It should be noted, however, that while the output feedback stability region can be chosen as close as desired to its state feedback counterpart by increasing the observer gain, the large observer gains result in poor performance due to noisy measurements. This however, cannot be mitigated simply by using a 'smaller' gain, because that would not preserve the stability guarantees. It cannot also be mitigated by using alternative estimation schemes (such as moving horizon estimators) that handle noise, but do not provide convergence guarantees. In practical scenarios, high gain observers can be used in a switched fashion–using a high gain initially for rapid convergence and then switching to a lower gain to mitigate noise. We also note that Theorem 3.3 provides a relation between the error bound (e_m), the time it takes to achieve such convergence (T_b) and the observer parameters and the value of the result is in exploiting this relationship to achieve convergence by as early a time as desired.

3.4.2 Output-feedback safe-parking of nonlinear process systems

Owing to the lack of full state measurements, the decision to utilize a safe parking candidate has to be made using only the available state estimates. This necessitates that the supervisor be able to make reliable inferences regarding the position of the states based upon the available state estimates. Proposition 1 below establishes the existence of a set, Ω_s, such that once the state estimation error has fallen below a certain value (note that the decay rate can be controlled by adjusting L_i), the presence of the state within the output feedback

stability region, Ω_b, can be guaranteed by verifying the presence of the state estimates in the set Ω_s. A similar notion was used in [57; 32] in the context of hybrid predictive control of linear systems and nonlinear switched systems under output feedback. The proof of Proposition 1 follows from the continuity of the function $V(\cdot)$, and relies on the fact that given a positive real number, δ_b, (i.e., given a desired output feedback stability region), one can find positive real numbers e_m and δ_s such that if the estimation error is below e_m (i.e., $\|x - \hat{x}\| \leq e_m$) and the estimate is within Ω_s (i.e., $V(\hat{x}) \leq \delta_s$ or $\hat{x} \in \Omega_s$), then the state itself must be within Ω_b, i.e., $V(x) \leq \delta_b$.

Proposition 1: *Given any positive real numbers δ_b and e_m, there exists a positive real number δ_s and a set $\Omega_s := \{x \in \mathbb{R}^n : V_i(x) \leq \delta_s\}$ such that if $\|x - \hat{x}\| \leq e$, where $e \in (0, e_m]$ then $\hat{x} \in \Omega_s \Longrightarrow x \in \Omega_b$.*

We are now ready to proceed with the design of safe parking framework under availability of limited measurements. To this end, consider the process of Eq.3.1 for which Assumptions 1 and 2 hold and, for each safe-parking point, an output feedback controller of the form of Eq.3.18 has been designed. Furthermore, given the desired output feedback stability regions $\Omega_{b,i} \subset \Omega_i$, $i = 1, \cdots, N$, we choose, for simplicity, $\epsilon_1 = \epsilon_2 = \cdots = \epsilon_n \leq \min\{\epsilon_i^*\}$ (i.e., the same observer gain is used for all candidate safe-park points). Also assume that the sets $\Omega_{s,i}$ and the times $T_{b,i}$ (see Assumption 2) have been determined, and let $T_b^{max} = \max\{T_{b,i}\}, i = 1, \cdots, N$. Theorem 3.4 below presents the output feedback safe parking framework.

Theorem 3.4 : *Consider the constrained system of Eq.3.1 under the MPC law of Eqs.3.5–3.8. If $x(0) \in \Omega_{b,n}$, $T^{fault} > T_b^{max}$ and $\hat{x}(T^{fault}) \in \Omega_{s,c}$ and $\Omega_c \subset \Omega_{b,n}$, then the switching rule*

$$u(t) = \left\{ \begin{array}{lll} u_{1,n} & , & 0 \leq t < T^{fault} \\ u_{2,x_c} & , & T^{fault} \leq t < T^{repair} \\ u_{1,n} & , & T^{repair} \leq t \end{array} \right\} \tag{3.23}$$

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

Proof of Theorem 3.4: The proof of the theorem follows along the lines of theorem 3.2.

If no fault takes place, practical stability of the nominal equilibrium point is guaranteed via Theorem 3.3. If a fault takes place, the key difference is the requirement of $T^{fault} > T_b$. This ensures that $|\hat{x}(T^{fault}) - x(T^{fault})| \leq e_m$. This in turn ensures that $\hat{x} \in \Omega_{s,c} \Rightarrow x \in \Omega_{n,c}$, that ensures practical stability of the equilibrium point x_c. Upon fault repair, and switching back to the original configuration, since $\hat{x} \in \Omega_c \in \Omega_{b,n}$ and $x \in \Omega_{b,n}$, practical stability of the nominal equilibrium point is achieved. To summarize, 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 3.4. □

Remark 3.9: Limited availability of state measurements requires a redesign of the controller (appropriately incorporating the state observer) as well as that of the safe-parking framework. In contrast to the state–feedback scenario, the decision to pick a safe-park point requires a time interval of at least T_b^{max}. This is done to ensure that the estimation error has enough time to decrease to a sufficiently small value such that, from that point in time onwards, the position of the state can be inferred by looking at the state estimate. Recall from Proposition 1 that the relation $\hat{x} \in \Omega_{s,j} \Longrightarrow x \in \Omega_{b,j}$ holds only when the estimation error is sufficiently small. Second, the decision to use a given safe-park point is not based on $\hat{x}$ being in the set $\Omega_{b,c}$; rather it is based on $\hat{x}$ being inside $\Omega_{s,c}$. The inference that $\hat{x} \in \Omega_{s,c} \Longrightarrow x \in \Omega_{b,c}$, however, can be made only once the error has dropped sufficiently, and this is guaranteed to happen after the closed–loop system has evolved fault-free at least for a time $T_b^{max} \geq T_{b,i}$. Therefore, the decision to go to a safe-park point is not made before an interval of length T_b^{max} elapses even if $\hat{x}$ resides in $\Omega_{s,c}$ at some earlier time. Note that in practice, if an actuator is prone to early faults, the observer design allows for decreasing the value of T_b^{max} to achieve earlier estimate convergence and allow for appropriate picking of the safe-park point.

Remark 3.10: Note that the proposed framework can be very well used to incorporate optimality considerations in the safe-parking framework. Specifically, having determined the appropriate safe-park points, the cost of transitioning to the safe-park point, the cost of operating at the safe-park point, as well as resuming nominal operation can be estimated using the auxiliary controller (see [36] for the incorporation of performance considerations in the state-feedback safe-parking framework). Furthermore, the contribution of the cost of

operation at the safe parking point 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 'weighted' 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 can be given increased weight.

Remark 3.11: Note that while the work in the present chapter develops the safe-parking framework for a single processing unit, the idea can very well be generalized to handle faults within a networked-plant setting. Specifically, operating considerations for downstream processing units can be incorporated in the choice of safe-park points for the upstream processing units. Additionally, the issue of handling sensor failures that may lead to loss of observability remains the topic of future work.

3.4.3 Illustrative simulation example: output feedback

We illustrate in this section the proposed safe-park framework under availability of limited measurements via the continuous stirred tank reactor (CSTR) of section 3.3.3. To this end, consider the CSTR example presented in section 3.3.3 in the absence of uncertainty and disturbances but subject to availability of limited measurements. Specifically, we now consider the case when only C_B and T_R are measured, that is $y_1 = T_R$, and $y_2 = C_B$. The relative degrees for the choice of process outputs, with respect to the vector of manipulated inputs, are $r_1 = 1$, and $r_2 = 2$, respectively. Therefore Assumption 1 is satisfied and an output feedback controller of the following form is designed.

$$\begin{aligned} \dot{\tilde{y}}_1^{(1)} &= L_1 a_1^{(1)} (y_1 - \tilde{y}_1^{(1)}) \\ \dot{\tilde{y}}_1^{(2)} &= \tilde{y}_2^{(2)} + L_2 a_1^{(2)} (y_2 - \tilde{y}_1^{(2)}) \\ \dot{\tilde{y}}_2^{(2)} &= L_2^2 a_2^{(2)} (y_2 - \tilde{y}_1^{(2)}) \end{aligned} \tag{3.24}$$

The observer parameters in the state estimator design of Eq.3.24 are chosen as $L_1 = L_2 = 100$, $a_1^{(1)} = a_1^{(2)} = 10$ and $a_2^{(1)} = a_2^{(2)} = 20$. The observer generates estimates of T_R as $\tilde{y}_1^{(1)}$ and of C_B and $\dot{C}_B$ as $\tilde{y}_1^{(2)}$ and $\tilde{y}_2^{(2)}$, respectively, to generate estimates of C_A.

Consider a scenario where the process starts from $F = (0.99\ Kmol/m^3,\ 394.02\ K)$ the observer is initialized at E = $(0.03\ Kmol/m^3,\ 424\ K)$, and the predictive controller drives the process toward the nominal operating point, $N = (0.45\ Kmol/m^3,\ 393\ K)$. Immediately, the heating valve fails, and reverts to the fail-safe position (completely shut) resulting in $Q_1 = 0\ KJ/s$. We first consider the case where the supervisor does not wait for a sufficient period of time in choosing the safe park point, and based on the proximity of the state estimates to the candidate safe-park point S_1, chooses $S_1 = (0.17\ Kmol/m^3, 424.75\ K)$ as the safe-park point. However, the process state is outside the stability region for the safe-park point 1, and the controller is unable to drive the process to the desired safe-park point. In contrast, if the supervisor waits for the estimates to converge, then the point S_2 $(0.8\ Kmol/m^3, 391.5\ K)$ is chosen as the safe-park point. Subsequently, the process is driven to and back from the safe park point after fault-repair (see solid lines in Fig.3.3). The state and input profiles are shown in Fig.3.4. In summary, the simulation scenario illustrates the necessity to appropriately design, and account for the presence of state estimation error in executing the safe-parking framework.

3.5 Application to the styrene polymerization process

In this section, we demonstrate the efficacy of proposed safe-parking mechanism to stabilize the styrene polymerization process described in Section 3.2.2, in presence of disturbances and measurement noise as well as availability of limited measurements. We consider errors in the values of the parameters A_p, hA and V_c of magnitude +1%, +2% and +10%, respectively as well as sinusoidal disturbances in the initiator flow rate F_i and the coolant inlet temperature T_{cf} of the form $+0.02F_{i,n}\sin(t/10)$ and $+0.1T_{cf,n}\sin(t/2)$ respectively, where the subscript n denotes the nominal steady–state value. It is assumed that measurements are available only for C_M and T (with sinusoidal measurement error of the form $+0.05C_{M,n}sin(t/4)$

and $+0.005T_c sin(t/4)$). The control objective is to stabilize the process at the nominal equilibrium point ($C_I = 0.07\ kmol/m^3$, $C_M = 3.97\ kmol/m^3$, $T = 303.55\ K$, $T_c = 297.95\ K$), corresponding to the nominal values of the manipulated inputs of $F_c = 1.31\ L/s$ and $F_m = 1.05\ L/s$, while handling disturbances/noise and a fault in the valve manipulating the coolant flow rate.

A high gain observer of the form of Eqs. 3.18 is designed, to estimate C_I and T_c from measurements of C_M and T, with parameters $L_1 = 10$, $L_2 = 40$, $a_1^{(1)} = 10$, $a_1^{(2)} = 20$, $a_2^{(1)} = 10$ and $a_2^{(2)} = 20$. To prevent the undesired effect of measurement noise, the measurements are filtered before passing on to the state observer. The predictive controller of Eqs.3.5–3.9 is designed using a quadratic Lyapunov function of the form $V(x) = x'Px$ with $P =$

$$\begin{bmatrix} 2091.4 & 35.9537 & -6.5924 & 9.1116 \\ 35.9537 & 1.1603 & -0.2231 & 0.3084 \\ -6.5924 & -0.2231 & 0.8473 & -0.2857 \\ 9.1116 & 0.3084 & -0.2857 & 1.4576 \end{bmatrix}$$

The first part of the simulation demonstrates the implementation of the output-feedback controller in the presence of uncertainty and measurement noise. To this end, consider the process starting from an initial condition ($C_I = 0.07\ kmol/m^3$, $C_M = 4.36\ kmol/m^3$, $T = 333.91\ K$, $T_c = 327.74\ K$) with the estimator initialized at the nominal equilibrium point. As seen by the dashed and solid lines in Fig.3.5 (see Fig.3.6 for the corresponding manipulated input profiles), the observer converges to the exact state values sufficiently fast and drives the process to the nominal equilibrium point.

We next demonstrate the implementation of the proposed safe-parking mechanism. To this end, consider the scenario, where after the process is stabilized at the nominal operating point, a fault occurs in coolant flow rate at $t = 83.3$ minutes, where the flow reverts to the fail safe value (of fully open, corresponding to $F_c = 31.31\ l/s$) and it is no longer possible to operate the process at the nominal equilibrium point. Subsequently, a safe-park point of ($C_I = 0.14\ kmol/m^3$, $C_M = 3.42\ kmol/m^3$, $T = 300.35\ K$, $T_c = 294.98\ K$) is chosen, and the process is driven to, and stabilized at the safe-parking point using the functioning control actuator. At $t = 150$ minutes the fault is rectified. The controller

subsequently uses both the functioning actuators and is able to drive the process back to the original nominal equilibrium point. In summary, the simulations demonstrate an application of the proposed safe-parking framework in the presence of limited (noisy) measurements, parametric uncertainty and disturbances.

3.6 Conclusions

This chapter considered the problem of handling actuator faults in nonlinear process systems subject to input constraints, uncertainty and limited availability of measurements. A framework was developed to handle faults that preclude the possibility of continued operating at the nominal equilibrium point using robust or reconfiguration-based fault-tolerant control approaches. First, we considered the presence of constraints and uncertainty and developed a robust Lyapunov-based model predictive controller as well as a safe-parking algorithm that preserves closed–loop stability upon fault repair. Specifically, a candidate parking point is chosen as 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 uncertainty), and 2) the safe-park candidate resides within the stability region of the nominal control configuration. Then we considered the problem of availability of limited measurements. An output feedback Lyapunov-based model predictive controller, utilizing an appropriately designed state observer (to estimate the unmeasured states), was formulated and its stability region explicitly characterized. An algorithm was then presented that accounts for the unavailability of the state measurements in the safe-parking framework. The proposed framework was illustrated using a chemical reactor example and demonstrated on a styrene polymerization process.

Table 3.1: Styrene polymerization parameter values and units.

F_i	=	0.3	L/s
F_m	=	1.05	L/s
F_s	=	1.275	L/s
F_t	=	2.625	L/s
F_c	=	1.31	L/s
$C_{If,n}$	=	0.5888	$kmol/m^3$
C_I	=	0.067	$kmol/m^3$
$C_{Mf,n}$	=	9.975	$kmol/m^3$
C_M	=	3.968	$kmol/m^3$
$T_{f,n}$	=	306.71	K
T	=	303.55	K
$T_{cf,n}$	=	294.85	K
T_c	=	297.95	K
A_d	=	5.95×10^{14}	s^{-1}
A_t	=	1.25×10^{10}	s^{-1}
A_p	=	1.06×10^8	$kmol/(m^3 \cdot s)$
E_d/R	=	14.897×10^3	K
E_t/R	=	8.43×10^2	K
E_p/R	=	3.557×10^3	K
f	=	0.6	
ΔH	=	-1.67×10^4	$kJ/kmol$
ρc_p	=	360	$kJ/(m^3 \cdot K)$
hA	=	700	$J/(K \cdot s)$
$\rho_c c_{pc}$	=	966.3	$kJ/(m^3 \cdot K)$
V_{pr}	=	3.0	m^3
V_c	=	3.312	m^3

Table 3.2: Chemical reactor parameters and steady–state values.

V	=	0.1	m^3
R	=	8.314	$KJ/(Kmol \cdot K)$
C_{A,in_s}	=	0.73	$Kmol/m^3$
T_{in_s}	=	310.0	K
Q_s	=	10.0	KJ/sec
ΔH	=	-4.78×10^4	$KJ/Kmol$
k_0	=	72×10^9	min^{-1}
E	=	8.314×10^4	$KJ/Kmol$
c_p	=	0.239	$KJ/(Kg \cdot K)$
ρ_f	=	1000.0	Kg/m^3
F	=	100×10^{-3}	m^3/min
T_{R_s}	=	393	K
C_{A_s}	=	0.447	$Kmol/m^3$

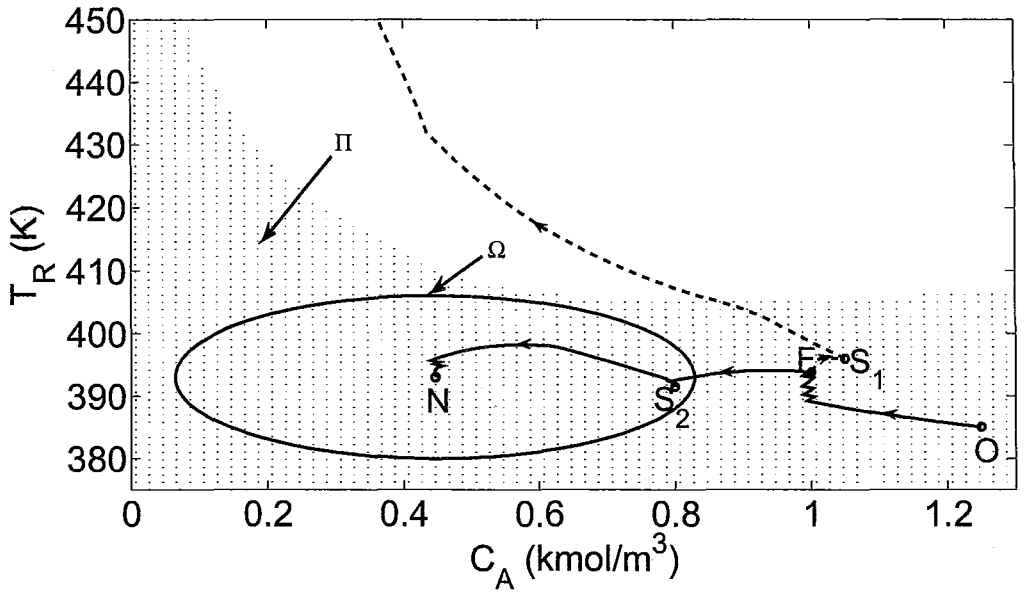

Figure 3.1: Evolution of the state trajectory for the CSTR example in the presence of uncertainty. Dashed line (- -) indicates the case when a safe-park point S_1 is arbitrarily chosen (resulting in the inability to resume nominal operation upon fault-repair) while the solid line (—) indicates the case when S_2 is chosen according to Theorem 2, guaranteeing resumption of nominal operation upon fault-repair.

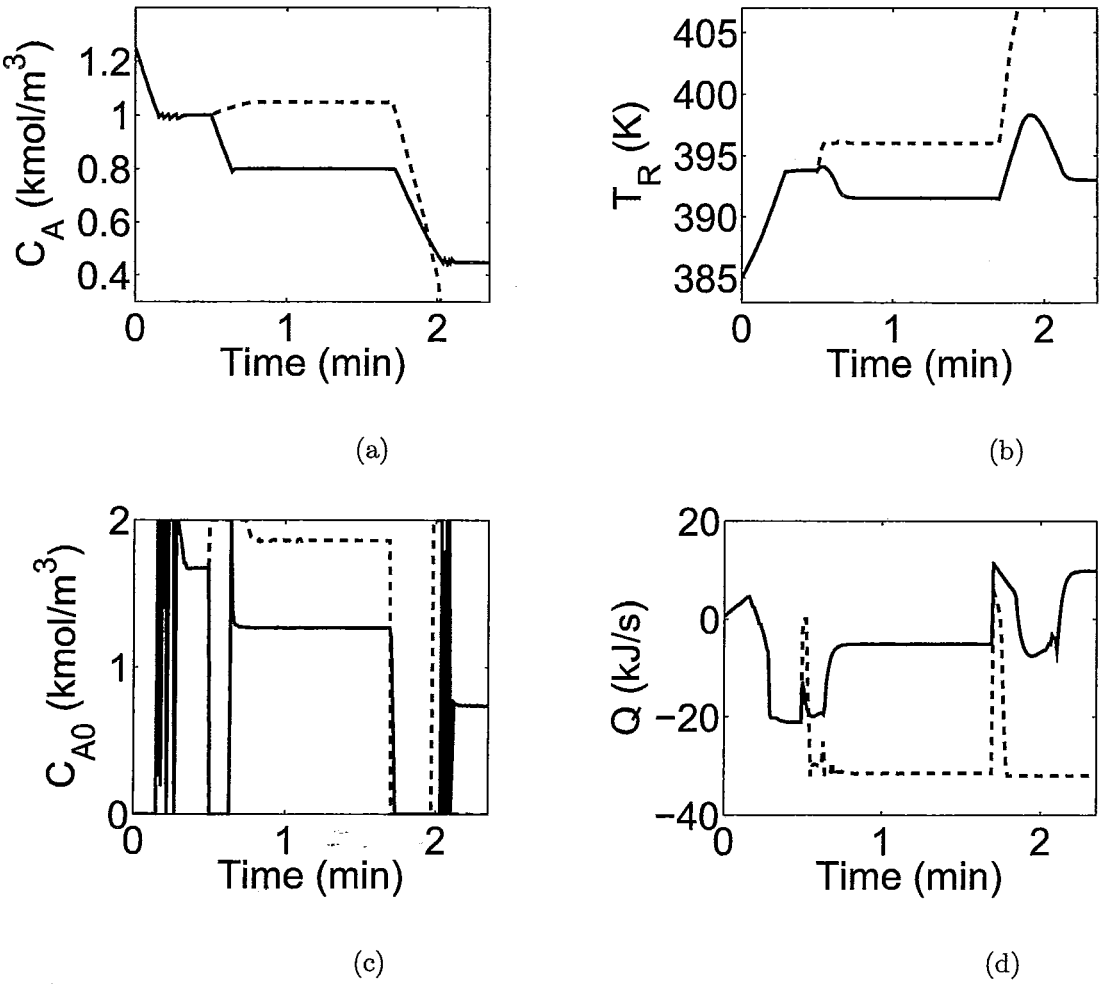

Figure 3.2: Evolution of the closed–loop state (a-b) and input (c-d) profiles for the CSTR example in the presence of uncertainty. Dashed lines (- -) indicate the case when a safe-park point S_1 is arbitrarily chosen (resulting in the inability to resume nominal operation upon fault-repair) while the solid lines (—) show the case when S_2 is chosen according to Theorem 2, guaranteeing resumption of nominal operation upon fault-repair.

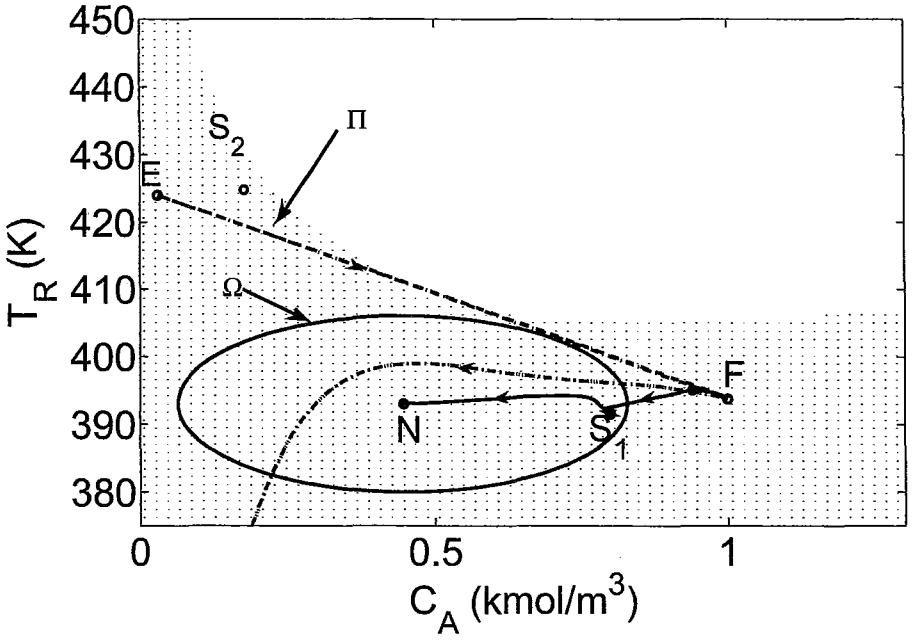

Figure 3.3: Evolution of closed–loop states and closed–loop state estimates for the CSTR example with limited availability of state measurements. The dashed–dot line (- .) and dotted line (...) represents the state estimates and state trajectories for the case when a safe-park point S_2 is immediately chosen, without waiting for the state estimates to converge, resulting in the inability to reach the chosen safe-park point. The dashed line (- -) and solid line (—) represents the state estimates and state trajectories for the case when a safe-park point S_1 is chosen after waiting for the convergence of the state estimates (utilizing Theorem 4), guaranteeing stabilization at the safe-park point and subsequent resumption of nominal operation upon fault-repair.

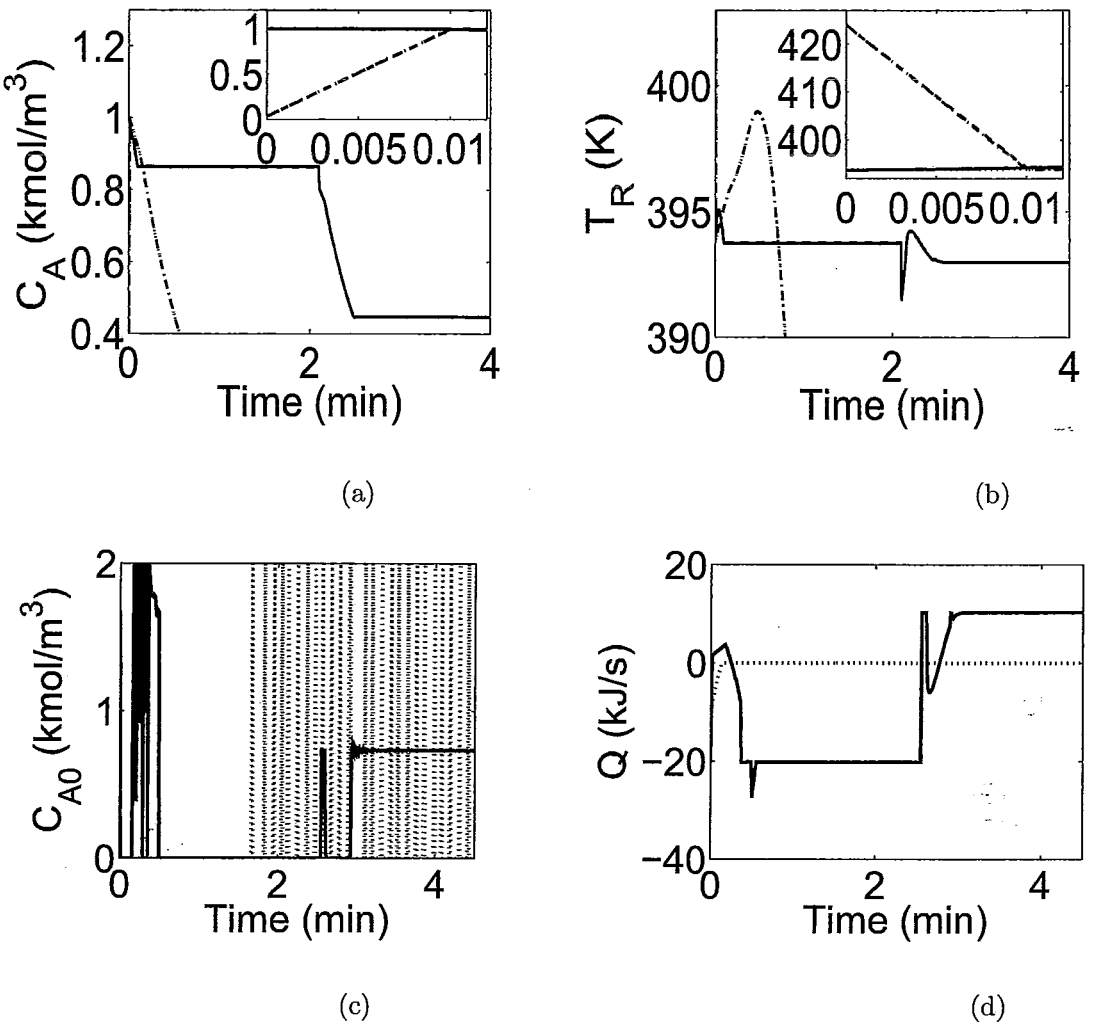

Figure 3.4: Evolution of the closed–loop state (a-b) and input (c-d) profiles for the CSTR example with limited availability of state measurements. The dashed–dot line (- .) and dotted line (...) represents the state estimates and state trajectories for the case when a safe-park point S_2 is immediately chosen, without waiting for the state estimates to converge, resulting in the inability to reach the chosen safe-park point. The dashed line (- -) and solid line (—) represents the state estimates and state trajectories (see the insets in (a) and (b) illustrating the convergence of the state estimates) for the case when a safe-park point S_1 is chosen after waiting for the convergence of the state estimates (utilizing Theorem 4), guaranteeing stabilization at the safe-park point and subsequent resumption of nominal operation upon fault-repair.

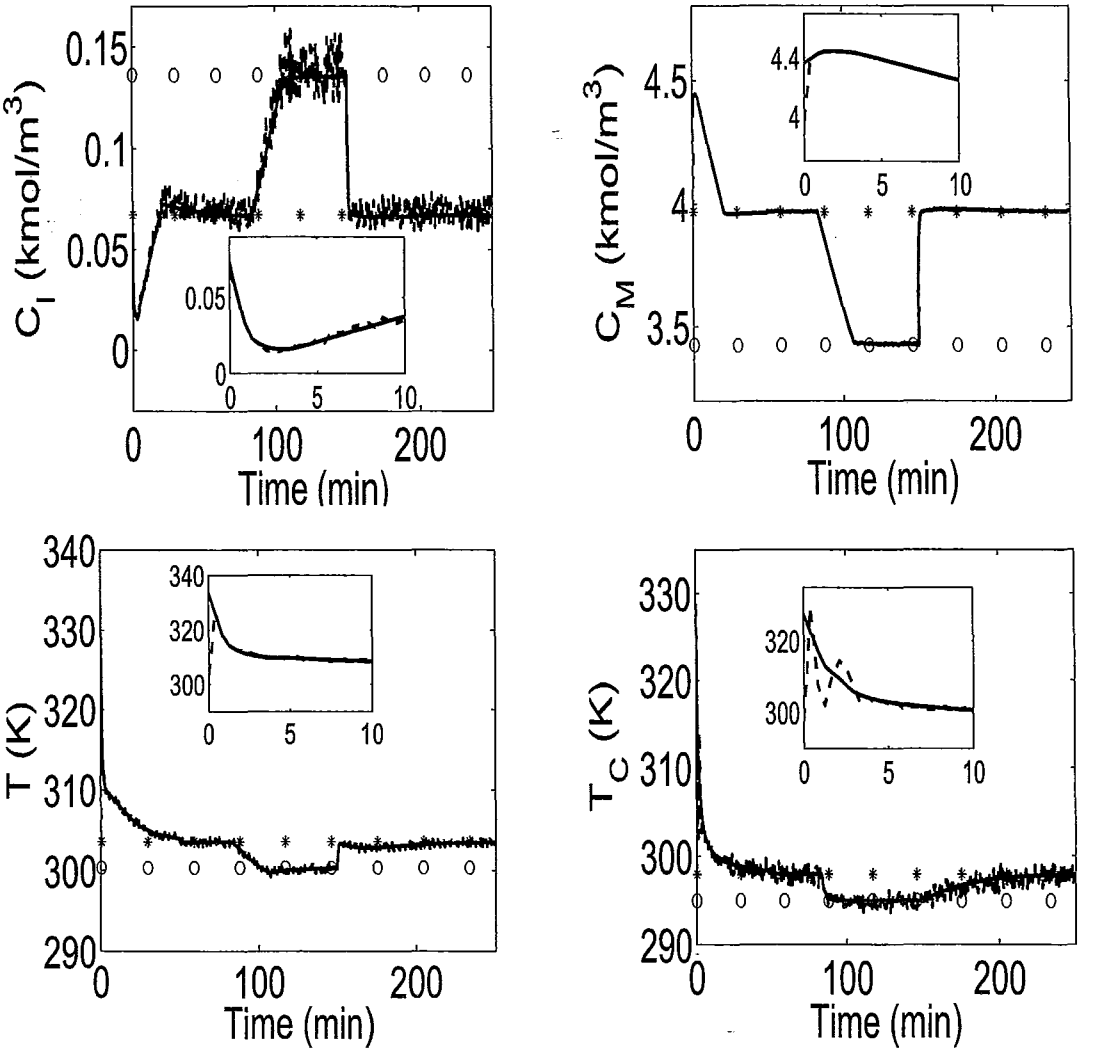

Figure 3.5: Evolution of the state (solid lines) and state estimates profiles (dashed lines) for the styrene polymerization process. Fault occurs at 83.3 min and is rectified at 150 min. The nominal operating point and the safe-park point are denoted by the markers $\star$ and o, respectively.

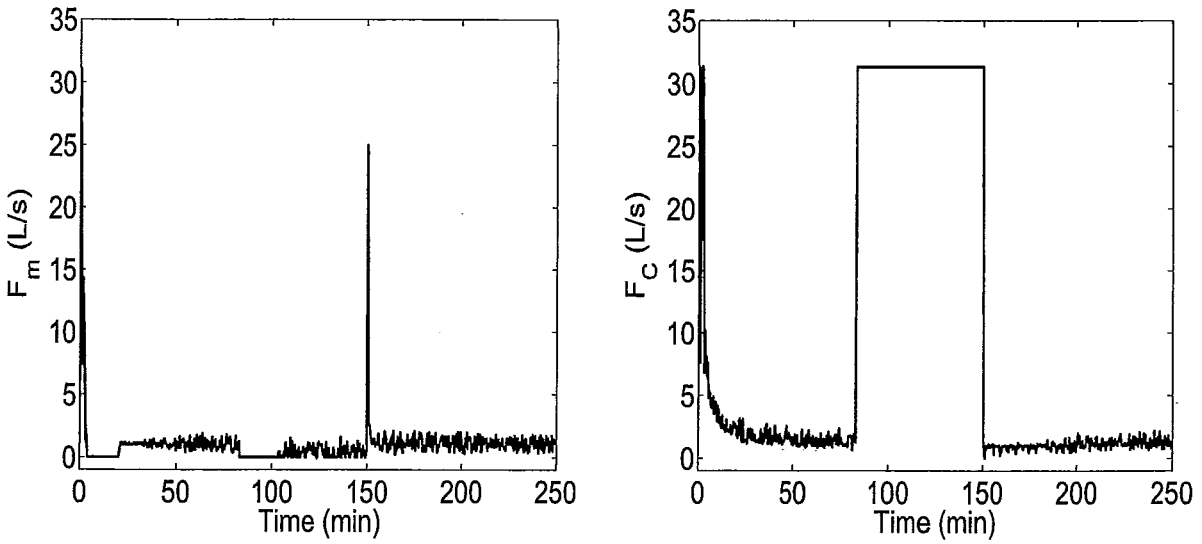

Figure 3.6: Evolution of input profiles for the styrene polymerization process. Fault occurs at 83.3 min and is rectified at 150 min. The nominal operating point and the safe-park point are denoted by the markers $\star$ and o, respectively.

Chapter 4

A Safe-Parking Framework for Fault-Tolerant Control of Transport-Reaction Processes

4.1 Introduction

Transport-reaction processes are characterized by significant convection and diffusion phenomena coupled with a chemical reaction. Such processes are essential in the production of various industrial products. Examples include tubular reactors and packed-bed reactors. For such processes, the distinguishing feature for the control problem is that it involves the regulation of distributed variables by using spatially-distributed control actuators and measurement sensors. The dynamic models of transport-reaction processes over finite spatial domains typically consists of highly dissipative partial differential equations (PDE), such as parabolic PDEs. These parabolic PDEs possess a highly dissipative differential operator which is characterized by an eigenspectrum which can be partitioned into a finite slow part and an infinite stable fast complement [35]. Due to the infinite-dimensional nature of the transport-reaction processes, the control designs for lumped parameter systems cannot be

directly implemented on transport-reaction systems.

To develop finite dimensional approximations of the infinite dimensional system for use in controller design, some of the existing approaches include discretizing the spatial domain (e.g, [9], [71]), which could possibly lead to high dimensional control designs, and exploiting the separation in the eigenspectrum of the parabolic operator via Galerkin's method. The reduced order model has been subsequently used to design nonlinear controllers for quasi-linear parabolic PDE systems (and other highly dissipative PDE systems, see e.g., [3] and the book [13] for details and references). These order reduction techniques have been used to design controllers for other classes of dissipative PDE systems, and address issues such as lack of full state measurement [8], uncertainty [14] and optimality [5]. Subsequently, the work in [26] has developed a general framework for the analysis and control of parabolic PDEs with input constraints via Lyapunov-based bounded controllers. To address the issue of state constraints satisfaction, Model Predictive Controllers (MPC) were designed using modal decomposition techniques [23; 21; 24]. In particular, the results in [23; 21; 24] addressed the problem of designing finite dimensional MPC formulations that ensure satisfaction of state constraints for the infinite dimensional system based on satisfaction of more stringent state constraints imposed on the finite dimensional system.

While MPC formulations with explicitly characterized stability regions are available for lumped parameter systems (see, e.g., chapter 2, [59]), an issue which has yet to be addressed for MPC of parabolic PDE systems is that of identifying, *a priori* (i.e., before controller implementation), the set of initial conditions of the infinite dimensional system from where feasibility of the optimization problem and closed-loop stability are guaranteed. Preparatory to the design of the safe-parking framework, one of the contributions of the work in the present chapter is to develop a Lyapunov-based MPC for the control of parabolic PDE systems modeled by parabolic PDEs that provides an explicit characterization of feasibility and therefore the stability region.

The stability guarantees of the control designs (including the proposed Lyapunov-based MPC), however, do not hold in the presence of actuator fault that prevents the imple-

mentation of the control action prescribed by the control law, and motivate the design of fault-tolerant approaches to preserve process stability and safety. Existing fault-tolerant approaches for distributed parameter systems shadow those of lumped parameter systems and follow the robust/reliable, or reconfiguration-based fault-tolerant control designs (see, e.g., [29; 25; 4]). Such approaches assume the availability of sufficient control effort or redundant control configurations to preserve operation at the nominal equilibrium point in the presence of faults (we will henceforth refer to operation at the nominal equilibrium point as 'nominal operation'). Specifically, within robust/reliable schemes, the robustness of the active control configuration is used to handle faults as disturbances (e.g., [84]). Reconfiguration-based approaches (see eg., [29; 30; 19]), on the other hand, assume the existence of a backup, redundant control configuration that can preserve nominal operation.

In contrast, handling faults which prevent the ability to operate at the nominal operating point has received limited attention. In particular, the case where a fault results in a scenario where the nominal operating point is no longer an equilibrium point for any allowable values of the functioning actuators has not been sufficiently addressed. Without a framework to handle such faults, ad-hoc approaches could result in the process being driven to a hazardous operating point, or to a state from where nominal operation cannot be resumed even upon fault-repair, thus resulting in a temporary shut down of the process which can have substantially negative economic ramifications.

Recently, in [36] a 'safe-parking' framework was developed that preserves process safety and enables smooth resumption of nominal operation on fault repair. This is accomplished by identifying appropriate 'safe-park' points where the process can be temporarily 'parked' until nominal operation can be resumed. In chapter 3 (also appeared in [51]), this safe-parking framework was generalized to handle the availability of limited measurements and the presence of disturbances and uncertainty. However, the safe-parking framework of chapter 3 and [36] considers lumped parameter systems described by ordinary differential equations (ODEs). In summary, the problem of designing a predictive controller which provides an explicitly characterized stability and feasibility region, along with a mechanism which handles faults that preclude the possibility of nominal operation has not been addressed for

transport-reaction processes described by parabolic PDE systems. Implementing control and fault handling schemes without accounting for the distributed nature of the process can lead to the inability to control and handle faults in the process. In particular, the stability guarantees of an MPC design based on lumped parameter approximation of the infinite dimensional system may not hold for the infinite dimensional system. Furthermore, a safe parking framework implemented without accounting for the infinite dimensional nature of the process could lead to the inability to preserve process safety and resume nominal operation.

Motivated by these considerations, this chapter addresses the problem of designing a Lyapunov-based predictive controller and handling actuator faults in quasi-linear parabolic PDEs subject to input constraints. To this end, by exploiting the separation of the eigenspectrum of the differential operator via Galerkin's method, a finite dimensional ODE system which captures the dominant dynamics of the PDE system is constructed. This ODE system is used as the basis for the synthesis of a Lyapunov-based predictive controller that enforces closed-loop stability and provides, simultaneously, an explicit characterization of the stability region. This predictive controller is then used to develop a safe-park framework which handles faults which preclude the ability to maintain nominal operation. The key idea in the safe-park framework is to operate the plant using the depleted control at an appropriate 'safe-park' location to prevent onset of hazardous situations as well as enable smooth resumption of nominal operation upon fault-repair. Specifically, a candidate parking location is termed a safe-park distribution 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. In determining the safe-park distribution, dynamic considerations (via stability regions) are incorporated over and above the steady state considerations (via determining existence of equilibrium distributions for acceptable values of the functioning actuators). The proposed framework is illustrated on a diffusion-reaction process.

4.2 Preliminaries

In this section, we describe the class of processes considered, and then employ model reduction techniques via Galerkin's method to derive a finite-dimensional system that captures the dominant dynamics of the infinite-dimensional system. This is followed by a motivating example of a diffusion-reaction process and then a formalization of the control problem.

4.2.1 Process description

In this chapter, we consider quasi-linear parabolic PDEs in one spatial dimension of the form:

$$\frac{\partial \bar{x}}{\partial t} = A\frac{\partial \bar{x}}{\partial z} + B\frac{\partial^2 \bar{x}}{\partial z^2} + wb(z)u_\rho + f(\bar{x}), \quad u_\rho(\cdot) \in \mathbf{U}_\rho \tag{4.1}$$

subject to the boundary conditions:

$$\begin{aligned} C_1\bar{x}(\alpha,t) + D_1\frac{\partial \bar{x}}{\partial z}(\alpha,t) &= R_1 \\ C_2\bar{x}(\beta,t) + D_2\frac{\partial \bar{x}}{\partial z}(\beta,t) &= R_2 \end{aligned} \tag{4.2}$$

and the initial condition:

$$\bar{x}(z,0) = \bar{x}_0(z) \tag{4.3}$$

where $\bar{x}(z,t) = [\bar{x}_1(z,t)\ldots\bar{x}_n(z,t)]^T$ denotes the vector of state variables, $z \in [\alpha,\beta] \subset \mathbb{R}$ is the spatial coordinate, $t \in [0,\infty)$ is the time, $u_\rho = [u^1\, u^2 \ldots u^m] \in \mathbb{R}^m$ denotes the vector of constrained manipulated inputs taking values in a nonempty convex subset $\mathbf{U}_\rho$ of $\mathbb{R}^m$, where $\mathbf{U}_\rho = \{u \in \mathbb{R}^m : u_{min,\rho} \leq u \leq u_{max,\rho}\}$, where $u_{min,\rho}, u_{max,\rho} \in \mathbb{R}^m$ denote the constraints on the manipulated inputs. $\frac{\partial \bar{x}}{\partial z}$, $\frac{\partial^2 \bar{x}}{\partial z^2}$ denote the first- and second-order spatial derivative of $\bar{x}$. $\bar{x}_0(z)$ denotes the initial condition, w is a constant, A, B, C_1, D_1, C_2, D_2 are constants matrices, R_1, R_2 are column vectors and $f(\bar{x})$ is a nonlinear vector function.

The vector $b(z)$ is a known smooth function of z of the form $b(z) = [b^1(z)\, b^2(z) \ldots b^m(z)]$, where $b^i(z)$ describes how the control action $u^i_\rho(t)$ is distributed in the finite spatial interval $[\alpha, \beta]$, and $\rho \in \{1, 2\}$ is a discrete variable that indexes the fault-free ($\rho = 1$) and faulty ($\rho = 2$) operation. Throughout the chapter, the notation $|\cdot|$ refers to the standard Euclidian norm in $\mathbb{R}^n$. The notation $L_\chi h$ denotes the standard Lie derivative of a scalar function $h(\cdot)$ with respect to the vector function $\chi(\cdot)$. We denote the nominal (possibly spatially-nonuniform) steady–state distribution, and nominal steady–state manipulated input values of Eq.4.1 as x^{nom}_{ss}, u^{nom}_{ss} respectively. Finally, we recall the definition of a class K and KL function. In particular, a function $\gamma_s : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is said to be class K if it is continuous, nondecreasing, and zero at zero. Similarly, a function $\beta : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is said to be of class KL if, for each fixed t, the function $\beta(s, \cdot)$ is continuous, increasing, and zero when $s = 0$ and, for each fixed s, the function $\beta(\cdot, t)$ is non-increasing and tends to zero as $t \to \infty$. The notation $X \backslash Y$, where X and Y are sets, refers to the relative complement, defined by $Y \backslash X = \{x \in Y : x \notin X\}$

We formulate the PDE of Eq.4.1 as an infinite dimensional system in the Hilbert space $\mathcal{H}([\alpha, \beta] : \mathbb{R}^n)$ with $\mathcal{H}$ being the space of functions defined on $[\alpha, \beta]$ that satisfy the boundary conditions of Eq.4.2, with inner product and norm:

$$(\omega_1, \omega_2) = \int_\alpha^\beta (\omega_1(z), \omega_2(z))_{\mathbb{R}} dz, \| \omega_1 \|_2 = (\omega_1, \omega_2)^{\frac{1}{2}} \tag{4.4}$$

where ω_1, ω_2 are two elements of $\mathcal{H}([\alpha, \beta]; \mathbb{R}^n)$ and the notation $(\cdot, \cdot)_{\mathbb{R}}$ denotes the standard inner product in $\mathbb{R}$. Defining the state function x on $\mathcal{H}([\alpha, \beta]; \mathbb{R}^n)$ as:

$$x(t) = \bar{x}(z, t), \quad t > 0, \quad z \in [\alpha, \beta] \tag{4.5}$$

the operator $\mathcal{A}$ as:

$$\mathcal{A}x = A\frac{\partial \bar{x}}{\partial z} + B\frac{\partial^2 \bar{x}}{\partial z^2}, \tag{4.6}$$

$$x \in D(\mathcal{A}) = \{x \in \mathcal{H}([\alpha, \beta], ; \mathbb{R}^n) : C_1 x(\alpha) + D_1 \frac{\partial x}{\partial z}(\alpha) = R_1, C_2 x(\beta) + D_2 \frac{\partial x}{\partial z}(\beta) = R_2\}$$

and the input operator as:

$$\mathcal{B}u = wbu \tag{4.7}$$

the system of Eqs.4.1-4.2-4.3 takes the form:

$$\dot{x} = \mathcal{A}x + \mathcal{B}u + f(x), \;\; x(0) = x_0 \tag{4.8}$$

where $f(x(t)) = f(\bar{x}(z,t))$, $x_0 = \bar{x}_0(z)$. We assume that the nonlinear terms $f(x)$ satisfy $f(0) = 0$ and are also locally Lipschitz continuous with respect to their arguments.

For $\mathcal{A}$, the eigenvalue problem is defined as:

$$\mathcal{A}\phi_j = \lambda_j \phi_j, \;\; j = 1, \ldots, \infty \tag{4.9}$$

where λ_j denotes an eigenvalue and ϕ_j denotes an eigenfunction; the eigenspectrum of $\mathcal{A}$, denoted by $\sigma(\mathcal{A})$, is defined as the set of all eigenvalues of $\mathcal{A}$, i.e. $\sigma(\mathcal{A}) = \{\lambda_1, \lambda_2, \ldots\}$. Assumption 1 that follows states an important property concerning the partition of the eigenspectrum of $\sigma(\mathcal{A})$ into slow and fast parts.

Assumption 1[13]:

1. $Re\{\lambda_1\} \geq Re\{\lambda_1\} \geq \cdots \geq Re\{\lambda_j\} \geq \cdots$, where $Re\{\lambda_j\}$ denotes the real part of λ_j
2. $\sigma(\mathcal{A})$ can be partitioned as $\sigma(\mathcal{A}) = \sigma_1(\mathcal{A}) + \sigma_2(\mathcal{A})$, where $\sigma_1(\mathcal{A})$ consists of the first m (finite) eigenvalues.
3. $Re\lambda_{m+1} < 0$ and $|Re\{\lambda_m\}|/|Re\{\lambda_{m+1}\}| = \mathcal{O}(\varepsilon)$ where $\varepsilon < 1$ is a small positive number.

Remark 4.1: The majority of diffusion-convection-reaction processes satisfy the assumption of countable eigenspectrum and the existence of a reduced sub-system that captures the dominant dynamics of the process (see example in Section 4.2.3, and chapter 4 in [13]). This property derives from the fact that the eigenspectrum of $\sigma(\mathcal{A})$ can be partitioned in two parts consisting of m slow, and infinite stable fast eigenvalues and is always satisfied by parabolic PDEs [35]. Note also that the sufficiency of a certain number of eigenmodes to capture the dominant dynamics of a PDE system can be empirically determined through computer simulation.

4.2.2 Galerkin's Method

In this section, a finite approximation to the infinite dimensional system in the form of a set of ODEs is derived by applying Galerkin's method to the system of Eq.4.1. Let $\mathcal{H}_s$, and $\mathcal{H}_f$ be modal subspaces of $\mathcal{A}$, defined as $\mathcal{H}_s = span\{\phi_1, \phi_2, \ldots, \phi_m\}$ and $\mathcal{H}_f = span\{\phi_{m+1}, \phi_{m+2}, \ldots, \}$. We note that the existence of $\mathcal{H}_s$, and $\mathcal{H}_f$ follows from Assumption 1. By defining orthogonal projection operators P_s and P_f as $x_s = P_s x$, $x_f = P_f x$, the state x of the system of Eq.4.8 can be decomposed as

$$x = x_s + x_f = P_s x + P_f x \tag{4.10}$$

The operators P_s and P_f are applied to the system of Eq.4.8 to derive an equivalent form of Eq.4.8 in terms of x_s and x_f:

$$\begin{aligned} \frac{dx_s}{dt} &= \mathcal{A}_s x_s + \mathcal{B}_s u + f_s(x_s, x_f), \\ \frac{\partial x_f}{\partial t} &= \mathcal{A}_f x_f + \mathcal{B}_f u + f_f(x_s, x_f), \\ x_s(0) = P_s x(0) = P_s x_0, \;\; & x_f(0) = P_f x(0) = P_f x_0 \end{aligned} \tag{4.11}$$

where $\mathcal{A}_s = P_s\mathcal{A}$, $\mathcal{B}_s = P_s\mathcal{B}$, $f_s = P_s f$, $\mathcal{A}_f = P_f\mathcal{A}$, $\mathcal{B}_f = P_f\mathcal{B}$ and $f_f = P_f f$ and partial derivative notation in $\frac{\partial x_f}{\partial t}$ is used to denote that the state x_f belongs to an infinite-dimensional space. In the above system, $\mathcal{A}_s$ is a diagonal matrix of dimension $m \times m$ of the form $\mathcal{A}_s = diag\{\lambda_j\}$, $f_s(x_s, x_f)$ and $f_f(x_s, x_f)$ are Lipschitz vector functions, and A_f is an unbounded differential operator which is exponentially stable (following from part 3 of Assumption 1 and the selection of $\mathcal{H}_s$, $\mathcal{H}_f$). In the remainder of the chapter, we will refer to the x_s-and x_f-subsystems in Eq.4.11 as the slow and fast subsystems, respectively. Neglecting the stable infinite-dimensional x_f-fast subsystem in the system of Eq.4.11, the following m-dimensional slow system is obtained:

$$\frac{d\bar{x}_s}{dt} = \mathcal{A}_s \bar{x}_s + \mathcal{B}_s u + f_s(\bar{x}_s, 0), \tag{4.12}$$

where the bar symbol in $\bar{x}_s$ denotes that this variable is associated with a finite-dimensional system. The system of Eq.4.12 will be referred to as the reduced system.

Remark 4.2: We note that empirical eigenfunction of the system in Eq.4.1 can be used within the procedure to develop the approximate ODE system in Eq.4.12, and it is not necessary that an analytical solution be available for the above eigenvalue problem. We also note that the choice of the basis functions $\{\phi_j\}$, $j = 1, \ldots, \infty$ is in principle not restricted to the solution of the above eigenvalue problem and can be any set of standard basis functions of $\mathcal{H}$. Specifically, eigenfunctions computed using Karhuen-Loeve (KL) expansion can be used as basis functions for the spaces $\mathcal{H}_f$, and $\mathcal{H}_s$ in place of the eigenfunctions of $\mathcal{A}$. Note also that a finite-dimensional approximation similar to that of Eq.4.12 could also be obtained by employing the methods of approximate inertial manifolds along with Galerkin's method (see chapter 4 in [13]).

4.2.3 Motivating example

In this section we present a benchmark diffusion-reaction process (used in [26] to demonstrate the implementation of the Lyapunov-based bounded control design) to motivate the control and fault handling safe-parking framework. To this end, consider a long, thin catalytic rod in a reactor. The inlet to the reactor is pure species A, and a zeroth-order exothermic reaction of the form $A \rightarrow B$ takes place on the rod. A cooling and heating medium in contact with the rod is used to control the rod temperature. The spatiotemporal evolution of the dimensionless rod temperature is described by the following parabolic PDE:

$$\frac{\partial \bar{x}}{\partial t} = \frac{\partial^2 \bar{x}}{\partial z^2} + \beta_T e^{\frac{-\gamma}{1+\bar{x}}} + \beta_U \left(\sum_{i=1}^{l} b_i(z) u_i(t) - \bar{x} \right) - \beta_T e^{-\gamma} \tag{4.13}$$

subject to the boundary and initial conditions:

$$\bar{x}(0,t) = 0, \qquad \bar{x}(\pi,t) = 0, \qquad \bar{x}(z,0) = \bar{x}_0(z), \tag{4.14}$$

where $\bar{x}$ denotes the dimensionless temperature, β_T denotes a dimensionless heat of reaction, γ denotes a dimensionless heat transfer coefficient, $u^i(t)$ denotes the i-th manipulated input which is the temperature of the cooling and heating medium, and $b_i(z)$ denotes the i-th actuator distribution function, chosen to be $b_i(z) = \delta(z - z_{ai})$ (i.e. a point-control actuator

influencing the rod at $z = z_{ai}$), where δ is the dirac-delta function. The following typical values of process parameters are used: $\beta_T = 50$, $\beta_U = 2$, $\gamma = 3$. We consider two-point actuators ($l = 2$) applied at $z_{a1} = \pi/3$, and $z_{a2} = 2\pi/3$. The solution of the eigenvalue problem for the above spatial differential operator can be solved analytically to yield

$$\lambda_i = -i^2, \qquad \phi_i(z) = \sqrt{\frac{2}{\pi}}\sin(iz), \qquad i = 1, \ldots, \infty, \tag{4.15}$$

Although the eigenvalues of the differential operator for this process are all stable, the exothermicity of the reaction lends to the instability of the steady–state corresponding to the nominal values of the manipulated inputs of $u^1 = -0.35$, and $u^2 = -0.45$ (i.e the system in Eq.4.13 linearized will have positive eigenvalues). The control objective is to stabilize the rod temperature profile at an unstable steady–state distribution $\bar{x}_{ss}(z,t)$ corresponding to the nominal values of the manipulated inputs of $u^1 = -0.35$, and $u^2 = -0.45$. The manipulated inputs are constrained as $-0.4 \leq u^1 \leq 1$, and $-1 \leq u^2 \leq 1$.

Consider the scenario where u^1, the manipulated input at $z = \pi/3$ fails and reverts to the fail-safe position (fully open). With the coolant temperature set to fully open, there simply does not exist an admissible value of the functioning manipulated input u_2, such that the nominal equilibrium distribution remains an equilibrium distribution for the process. Hence, this precludes the possibility of continued operation at the nominal equilibrium point (regardless of the choice of the control law).

The key problem is twofold; First, a Lyapunov-based model predictive controller which can handle input constraints, and provide an explicit characterization from where stabilization can be achieved for the infinite-dimensional system must be designed. Upon failure of a control actuator, by utilizing this predictive control design we must determine how to operate the process to maintain process safety and, upon fault-repair, efficiently resume nominal operation.

4.2.4 Problem formulation and solution overview

In this chapter, we first consider the problem of designing an MPC that provides an explicit characterization of the stability region. Next, we consider faults in the control actuators which by assumption revert to a fail-safe position upon failure. Examples of fail-safe positions include fully open for a valve regulating a coolant flow rate, fully closed for a valve regulating a steam flow etc. Specifically, we assume that a fault occurs (without loss of generality), in the first control actuator $u^1(t)$ at a time T^{fault} and reverts to a fail-safe position, and is subsequently rectified at a time T^{repair} (i.e., for $t \leq T^{fault}$ and $t > T^{repair}$, $\sigma(t) = 1$ and $\sigma(t) = 2$ for $T^{fault} < t \leq T^{repair}$), as $u_2^1(t) = u_{failed}^1$, with $u_{min,2}^1 \leq u_{failed}^1 \leq u_{max,2}^1$, where u^i denotes the ith component of a vector u, for all $T^{fault} < t \leq T^{repair}$, leaving only u_2^i, $i = 2 \ldots m$ available for feedback control. Note that if $u_{failed}^1 \neq u_{ss}^{1^{nom}}$, i.e., if the failed actuator is frozen at a non-nominal value, then the process may not be able to be stabilized at the nominal equilibrium distribution using the remaining functioning control actuators. In other words, in the event that one of the the manipulated input fails and reverts to a fail-safe position, it may happen that no admissible combination of the functioning inputs exists for which the nominal equilibrium distribution continues to be an equilibrium distribution. In such a scenario, an attempt to continue operation at the nominal operating distribution will result in the process being stabilized at a non-nominal distribution which may result in the onset of hazardous or undesirable process conditions. In addition, a decision to drive the process state to an arbitrarily chosen distribution may result in the inability to resume nominal operation upon fault-repair. We will denote the set of possible steady-state distributions as the candidate safe-park set:

$$X_{sp} := \{x_{sp} \in D(\mathcal{A}) : \mathcal{A}x_{sp} + f(x_{sp}) + b^1 u_{failed}^1 + \textstyle\sum_{i=2}^{m} b^i u_2^i = 0,\ u_{min}^i \leq u_2^i \leq u_{max}^i, i = 2, \ldots, m\} \tag{4.16}$$

Each candidate safe-park distribution represents a possible steady–state distribution corresponding to the actuator fail-safe position, and the other manipulated inputs at acceptable values. We define the safe-parking problem as the one of identifying safe-park distributions $x_{sp} \in X_{sp}$ that preserve process safety and allow smooth resumption of nominal operation upon fault-repair.

4.3 Lyapunov-based model predictive control of parabolic PDE systems

Preparatory for use within the safe-parking framework, in this section, the finite dimensional system derived in Section 4.2.2 is used to design a Lyapunov-based model predictive controller that accounts for the discrete nature of implementation of the controller and provides an explicit characterization of the set of initial conditions from where the optimization problem in the predictive controller is guaranteed to be initially and successively feasible.

4.3.1 Controller design and analysis

Having obtained a finite-dimensional system that approximates the dominant dynamics of the infinite-dimensional system, we proceed to develop a Lyapunov-based predictive controller. This controller design, for each mode of operation (we drop the subscript ρ for ease of notation) will enforce closed-loop stability of the infinite-dimensional system, provide an explicitly characterized feasibility and stability region, and fully exploit the constraint handling capabilities of the predictive control approach. To this end, consider the system of Eq.4.12 for which a predictive controller is designed. Using a control Lyapunov function $V : \mathbb{R}^n \rightarrow \mathbb{R}$ we define the set:

$$\Pi^d = \{x_s \in \mathbb{R}^n : \inf_{u \in \mathbf{U}} L_f V(x_s) + L_G V(x_s) u \leq -\epsilon^*\} \cup \{x_s \in \mathbb{R}^n : |x_s| \leq d\} \qquad (4.17)$$

where d, and ϵ^* is a parameter to be defined later. Thus for all values of the state in the set Π^d, there exists a value of the manipulated input that satisfies the input constraints (note that the definition of the set Π^d does not depend on any specific control law, but only on the Lyapunov function, the process dynamics, and input constraints and d) and also achieves negative definiteness of the Lyapunov function derivative. Furthermore, we define the sets:

$$\Omega_c := \{\bar{x}_s \in \mathbb{R}^n : V(\bar{x}_s) \leq c\} \qquad (4.18)$$

for a given $c > 0$. Let c^{max} be the largest number for which $\Omega_{c^{max}} \subseteq \Pi^d$.

Consider now the formulation of the predictive controller designed on the basis of the low-order, finite dimensional reduced slow subsystem describing the evolution of the $\bar{x}_s$ states (the fast subsystem is neglected). The receding horizon implementation of the control action is computed by solving an optimization problem of the form:

$$u_{MPC}(\bar{x}_s, x_{ss}^{nom}, u_{min}, u_{max}) \;=\; argmin\{J(\bar{x}_s, t, u(\cdot))|u(\cdot) \in S\} \tag{4.19}$$

$$s.t.\;\; \frac{d\bar{x}_s}{dt} = \mathcal{A}_s\bar{x}_s + \mathcal{B}_s u + f_s(\bar{x}_s, 0) \tag{4.20}$$

$$\dot{V}(\bar{x}_s(\tau)) \leq -\epsilon^* \;\; \forall\, \tau \in [t, t+\Delta)\; if \;\; V(\bar{x}_s(t)) > \delta' \tag{4.21}$$

$$V(\bar{x}_s(\tau)) \leq \delta' \;\forall\, \tau \in [t, t+\Delta) \;\; if \;\; V(\bar{x}_s(t)) \leq \delta' \tag{4.22}$$

$$\bar{x}_s(t+\tau) \;\; \in \;\; \Pi^d \;\; \forall\, \tau \in [t, t+\Delta) \tag{4.23}$$

where $u_{MPC}(\bar{x}_s, x_{ss}^{nom}, u_{min}, u_{max})$ is the Lyapunov based model predictive controller designed to stabilize the process at x_{ss}^{nom} with constraints on the inputs as $u_{min} \leq u(t) \leq u_{max}$ (defined by the set U), $S = S(t,T)$ is the family of piecewise constant functions (functions continuous from the right), with period Δ, mapping $[t, t+T]$ into U and T is the horizon. Eq.4.20 is the reduced finite-dimensional model, V is a control Lyapunov function and δ', ϵ^* are parameters to be determined.The performance index is given by

$$J(\bar{x}_s, t, u(\cdot)) \;=\; \int_t^{t+T} \left[\|\bar{x}_s^u(\theta; \bar{x}_s, t)\|_Q^2 + \|u(s)\|_R^2\right] d\theta \tag{4.24}$$

where Q is a positive semi-definite symmetric matrix and R is a strictly positive definite symmetric matrix. $\bar{x}_s^u(\theta; \bar{x}_s, t)$ denotes the solution of Eq.4.12, due to control u, with initial state $\bar{x}_s$ at time t. The minimizing control $u^0(\cdot) \in S$ is then applied to the plant over the interval $[t, t+\Delta)$ and the procedure is repeated indefinitely. Since the reduced order system of Eq.4.12 comprises of a finite set of ODEs, one can use the result from chapter 2, to show the stability and feasibility properties of the closed–loop reduced order system under the implementation of this predictive control formulation (this is formalized in part 1 of Theorem 4.1 below). Specifically, it can be shown that the set $\Omega_{c^{max}}$ is an estimate of the stability region for the reduced order system of Eq.4.12, and if $\bar{x}_s(0) \in \Omega_{c^{max}}$, then

$\bar{x}_s(t) \in \Omega_{c^{max}}$, $\forall t \geq 0$ under the implementation of the above MPC law. These stability properties for the reduced order system are subsequently used in part 2 of the Theorem 4.1 below to show the practical stability of the infinite-dimensional system of Eq.4.1.

Theorem 4.1 : *(1) Consider the system of Eq.4.12 under the MPC law of Eqs.4.19-4.24. Then, given any positive real number d, there exist positive real numbers δ', ϵ^*, and Δ^*, such that if $\bar{x}_s(0) \in \Omega_{c^{max}}$, where $\Omega_{c^{max}}$ was defined in Eq.4.18, and $\Delta \in (0, \Delta^*]$, then the optimization problem of Eq.4.19-4.24 is feasible for all times, $\bar{x}_s(t) \in \Omega_{c^{max}}$, $\forall t \geq 0$, and the closed-loop system is practically stable in the sense that $\limsup_{t\to\infty} |\bar{x}_s(t)| \leq d$. Furthermore, if $\bar{x}_s(0) \in \Pi^d \backslash \Omega_{c^{max}}$, then if the optimization problem is feasible for all times, then $\bar{x}_s(t) \in \Pi^d$,$\forall t \geq 0$, and $\limsup_{t\to\infty} |\bar{x}_s(t)| \leq d$.*
(2) Consider the parabolic PDE system of Eq.4.1, for which Assumption 1 holds, under the MPC law of Eqs.4.19-4.24. Then, given any positive real numbers d^s, and δ_f, there exists positive real numbers δ', ϵ^*, Δ^*, s and ε^* such that if $x_s(0) \in \Omega_s$, where Ω_s was defined in Eq.4.18, $\|x_f(0)\|_2 \leq \delta_f$, $\Delta \in (0, \Delta^*]$, and $\varepsilon \in (0, \varepsilon^*]$, the infinite-dimensional closed-loop system is practically stable in the sense that $\limsup_{t\to\infty} |x_s(t)| \leq d^s$ and $\limsup_{t\to\infty} \|x_f(t)\|_2 \leq d^s$.

Proof of Theorem 4.1: *Part 1:* Since the system of Eq.4.12 is composed of a m-dimensional finite set of ODEs, the proof of this part is similar to the proof of Proposition 2 of [58]. Using a similar argument it can be established that given a positive real number, d, there exists an admissible manipulated input trajectory, and values of Δ^*, and δ', such that for any $\Delta \in (0, \Delta^*]$ and $\bar{x}_s(0) \in \Omega_{c^{max}}$, the optimization problem is s feasible for all times, $\limsup_{t\to\infty} |V(\bar{x}_s(t))| \leq \delta'$, and $\limsup_{t\to\infty} |\bar{x}_s(t)| \leq d$. In preparation for part 2 of the theorem we briefly state an equivalent form of this result in terms of comparison functions. It follows that for all $\bar{x}_s(0) \in \Omega_{c^{max}}$, there exists a class KL function β_s, and a class K function γ_s, such that the closed–loop reduced order system under the MPC law of Eqs.4.19–4.24 satisfies

$$|\bar{x}_s(t)| \leq \beta_s(|\bar{x}_s(0)|, t) + \gamma_s(\Delta), \tag{4.25}$$

for all times $t > 0$, where $\gamma_s(\Delta^*) = d$.

Part 2: The proof of this part initially follows similar lines as Theorem 4.1 in [26], where

the two time scale nature of the system is exploited with the aid of singular perturbed arguments. However, the present argument differs from Theorem 4.1 in [26] in that it accounts for the discrete implementation of the control action. Substituting the predictive controller of Eqs.4.19–4.24 into Eq.4.11 and using the separation of the eigenspectrum of parabolic operator we can represent the closed–loop system in singularly perturbed form. This follows since $\varepsilon = |Re\lambda_1|/|Re\lambda_{m+1}|$, and $0 < \varepsilon \ll 1$ (Assumption 1, part 3) [14]. Hence, Eq.4.11 can be written as follows:

$$\begin{aligned} \frac{dx_s}{dt} &= \mathcal{A}_s x_s + \mathcal{B}_s u_{MPC} + f_s(x_s, 0) + [f_s(x_s, x_f) - f_s(x_s, 0)], \\ \varepsilon \frac{\partial x_f}{\partial t} &= \mathcal{A}_{f\varepsilon} x_f + \varepsilon \bar{f}_f(x_s, x_f), \end{aligned} \tag{4.26}$$

where $\mathcal{A}_{f\varepsilon}$ is an unbounded differential operator defined as $\mathcal{A}_{f\varepsilon} = \varepsilon \mathcal{A}_f$ and $\bar{f}_f(x_s, x_f) = \mathcal{B}_f u_{MPC} + f_f(x_s, x_f)$. Note that $f_f(x_s, x_f)$ is independent of ε. In this case, x_s represents the slow states, and x_f represents the fast states. Introducing the fast time scale $\tau = t/\varepsilon$ and setting $\varepsilon = 0$, we obtain the following infinite-dimensional fast subsystem:

$$\frac{\partial \bar{x}_f}{\partial \tau} = \mathcal{A}_{f\varepsilon} \bar{x}_f, \tag{4.27}$$

where the bar symbol in $\bar{x}_f$, denotes that the state $\bar{x}_f$ is associated with the approximation of the fast x_f-subsystem. Since $Re\lambda_{m+1} < 0$ (Assumption 1) and using the definition of ε, we have that the above system is globally exponentially stable. Therefore there exists real numbers $k_1 \geq 1$, $a_1 > 0$ such that

$$\|\bar{x}_f(\tau)\|_2 \leq k_1 \|\bar{x}_f(0)\|_2 e^{-a_1 \tau}, \quad \forall \tau \geq 0. \tag{4.28}$$

Setting $\varepsilon = 0$ in the system of Eq.4.26 and using the fact that the operator $\mathcal{A}_{f\varepsilon}$ is invertible, we have that the steady–state solution of the $\bar{x}_f$ subsystem is $\bar{x}_{fss} = 0$. The finite-dimensional closed-loop slow system therefore reduces to the one analyzed in part 1 of the theorem. This has already been shown to be practically stable (x_s will asymptotically reach any arbitrary small neighborhood about the origin of small d) for all initial conditions within $\Omega_{c^{max}}$, and $\Delta \in (0, \Delta^*]$.

Let $r^{max} = \max_{V(x) \leq c^{max}} |x|$. It follows that,

$$V(x) \leq c^{max} \Rightarrow |x| \leq r^{max}$$

Let r^s be a positive real number such that $\beta_s(r^s, 0) + \gamma_s(\Delta^*) + d' < r^{max}$ for the class KL function β_s, and class K function γ_s given in the proof of part 1, and for a $d' > 0$ which to be defined later. We let s to be the largest positive number such that

$$V(x) \leq s \Rightarrow |x| \leq r^s \tag{4.29}$$

Using the stability properties for the fast and slow subsystems, and using the fact that there exists some r^{max}, such that $|\bar{x}_s(0)| \leq r^{max}$ for all $\bar{x}_s(0) \in \Omega_{c^{max}}$, it can be shown, with the aid of calculations similar to those preformed in [17], that if the eigenvalue separation parameter ε is small enough, the trajectories of the infinite-dimensional closed-loop system are bounded. That is, for any given d', d, and δ_f, there exists positive real numbers δ', Δ^*, s and ε^* such that if $x_s(0) \in \Omega_s$, $\|x_f(0)\|_2 \leq \delta_f$, $\Delta \in (0, \Delta^*]$, and $\varepsilon \in (0, \varepsilon^*]$, then the following inequalities hold for $t \geq 0$:

$$\begin{aligned} |x_s(t)| &\leq \beta_s(|x_s(0)|, t) + d + d', \\ \|x_f(t)\|_2 &\leq \beta_f(\|x_f(0)\|_2, t/\varepsilon) + d'. \end{aligned} \tag{4.30}$$

where β_s, and β_f are class KL functions, and d is the same as in part 1 of the Theorem. Note the definition of Ω_s as stated in Eq.4.29 requires that x_s be within $\Omega_{c^{max}}$, and also satisfy $\beta(|x_s(0)|, 0) + \gamma_s(\Delta^*) + d' \leq r^{max}$. Note that since $\beta(s, 0) \geq s$, for all $s \in \mathbb{R}$, it follows that $r^{max} > r^s$. The inequalities in Eq.4.30 ensure that the "slow" states of the closed-loop system remain within $\Omega_{c^{max}}$, and thus preserving the the feasibility of the optimization problem in Eqs.4.19–4.24. Note that the bound on the state trajectories given by Eq.4.30 will ultimately depend on d and d'. Since both d and d' are arbitrary, we can choose both to be small enough such that after a sufficient time, say $\tilde{t}$, the trajectories of the closed-loop system are confined within a small compact neighborhood of the origin. This time $\tilde{t}$, is dependent on both the initial condition and the desired size of the neighborhood, but not on ε. Choose $d = d^s/4$, and $d' = d^s/4$, then let $\tilde{t}$ be the smallest time such that $\max\{\beta_s(|x_s(0)|, \tilde{t}), \beta_f(\|x_f(0)\|_2, \tilde{t}/\varepsilon)\} \leq d^s/2$. Then it can be easily verified that

$$|x_s(t)| \leq d^s, \;\; \|x_f(t)\|_2 \leq d^s, \;\; \forall t \geq \tilde{t} \tag{4.31}$$

Therefore it follows, that $\limsup_{t\to\infty} |x_s(t)| \leq d^s$ and $\limsup_{t\to\infty} \|x_f(t)\|_2 \leq d^s$. This completes the proof of Theorem 4.1. □

Remark 4.3: Note that for all initial conditions in the set $\Omega_{c^{max}}$, the above MPC law is guaranteed to achieve negative definiteness of the time-derivative of the Lypaunov function along the trajectories of the finite-dimensional closed-loop reduced order system for all times, while satisfying input constraints. Therefore, the set $\Omega_{c^{max}}$ represents an estimate of the stability region for the closed-loop system of Eq.4.12. By exploiting the large separation of slow and fast eigenmodes of the parabolic operator in Eq.4.1, the estimate of the closed–loop stability region for the finite reduced-order system is practically preserved for the closed–loop infinite dimensional system of Eq.4.1. Specifically, given any initial "slow" state within a subset of $\Omega_{c^{max}}$, and any initial "fast" state, there exists ε^* (the minimum required separation in the eigenmodes), ϵ^* (the minimum required decay rate of the Lyapunov function), and Δ^* (the maximum implement and hold time) such that the MPC law of Eqs.4.19–4.24 continues to enforce practical stability in the constrained infinite dimensional closed–loop system. Theorem 1 above establishes that for all initial states within Ω_s, the above MPC law ensures that, during the evolution of the state, the "slow" component of the state remain within $\Omega_{c^{max}}$. Note that the fact that the stability region is only practically preserved can be attributed to the nonlinear terms $f_s(x_s, x_f)$ and $f_f(x_s, x_f)$ in Eq.4.11. The nonlinear terms introduce an interconnection between the two subsystems resulting in a slight mismatch (dependent on the separation in the eigenmodes) between the slow states of the reduced finite-dimensional subsystem and the slow states of the infinite-dimensional subsystem. The absence of these nonlinear terms (as in [21; 24]), would result in the exact preservation of the stability region.

Remark 4.4: The work in [26], and [29] (in the context of switched systems) utilize a similar decomposition technique to design stabilizing nonlinear bounded laws that establishes closed–loop asymptotic stability of the constrained infinite-dimensional system while also providing an explicit characterization of the sets of admissible initial conditions which guarantee closed-loop stability. The above developed MPC recognizes discrete implementation of the MPC and accordingly achieves practical stability. That is, the state profile reaches a small neighborhood of the origin (the size of which depends on the implement and hold time Δ, and the required rate of the Lyapunov function decay ϵ^*). Note that this is not a limitation of the MPC formulation, but is due to the discrete–time implementation of

the predictive control formulations. The same practical stability would be achieved in the discrete–time implementation of any other control law as well. Furthermore, the constraint in Eq.4.23, by requiring the states to remain in the region from where negative definiteness of $\dot{V}$ is achievable, enhances the set of initial conditions (compared to the Lyapuonv-based bounded control designs) from where closed–loop stability is achieved (see [52] for further discussion on this issue).

Remark 4.5: An estimate of ε^* (the minimum necessary separation between the slow and fast eigenvalues) can in principle be obtained from proof of Theorem 4.1 via singular perturbation techniques. However, this estimate is typically conservative. To alleviate this conservatism, computer simulations can be preformed to obtain a better estimate of ε^*. Specifically, for an initial condition in $\Omega_{c^{max}}$ from where the proposed predictive controller with a certain number of modes is unable to achieve closed-loop stability, the simulations have to be repeated with gradual increases in the number of modes used within the control design (reduced-order system) until closed-loop stability is achieved. The separation parameter corresponding to the number of modes required to achieve closed–loop stability from this initial condition could serve as a better estimate for ε^*.

Remark 4.6: The MPC formulations developed in [23] and [24] are similar to the formulation developed in this work in that they utilize the separation of the eigenspectrum of the parabolic operator to establish a reduced order model which can be used within the predictive controller. The results in [23; 24], however, focused on the issue of state constraint satisfaction, and under the assumption of initial feasibility, determined the appropriate 'backing off' from the constraint that must be incorporated in the control design using the reduced order model, such that constraint satisfaction for the infinite dimensional system is achieved. In contrast, the present formulation, while not considering state constraints, focuses on the satisfaction of input constraints, and appropriately designed 'stability constraints' and provides *a priori* the set of initial conditions of the infinite-dimensional system from where feasibility of the optimization problem is guaranteed and constrained stabilization of the closed-loop system can be established. The key idea from the results in [23; 24] and the work in the present chapter can very well be amalgamated to simulta-

neously achieve state constraint satisfaction and explicitly characterize the set of initial conditions from where the optimization is feasible.

4.3.2 Implementing the Lyapunov-based MPC on the diffusion-reaction process

In this section, we apply the predictive control formulation from section 4.3.1, to the diffusion-reaction process of Eqs.4.13-4.14. To derive a finite dimensional approximation of the process, we first note that the linearization of Eq.4.13 around the unstable steady–state distribution $\bar{x}_{ss}(z,t)$ corresponding to the nominal values of the manipulated inputs of $u^1 = -0.35$, and $u^2 = -0.45$, possesses two unstable eigenvalues. Therefore we take the first two eigenvalues to be dominant and use the aforementioned Galerkins method to derive a second order approximate model. To simplify the presentation of our results, we will work in an equivalent representation of the system in Eq.4.1 in terms of evolution of the amplitudes of the eigenmodes.

$$\dot{\bar{a}}_s(t) = A_s\bar{a}_s(t) + f(\bar{a}_s) + B_s(z)u(t) \tag{4.32}$$

where $\bar{a}_s(t) = [\bar{a}_1(t)\ \bar{a}_2(t)]'$, where $\bar{a}_i(t) \in \mathbb{R}$, $A_s = diag\{\lambda_i\}$, where λ_i is the eigenvalue given in Eq.4.15, $B_s(z)$ is a matrix whose i-th row is of the form $\beta_U[\phi_i(\pi/3)\ \phi_i(2\pi/3)]$, $u(t) = [u^1(t)\ u^2(t)]'$, $\bar{x}_s(t) = \sum_{i=1}^{2} \bar{a}_i(t)\phi_i(t)$ and $f(\bar{a}_s) = [\bar{f}_1\ \bar{f}_2]$. The nonlinear function $\bar{f}_i$ is given by $\bar{f}_i = (\tilde{f}_i, \phi_i(z))$, where $\tilde{f}_i = \beta_T e^{\frac{-\gamma}{1+\bar{x}_s}} - \beta_U\bar{x}_s - \beta_T e^{-\gamma}$. The ODE in Eq.4.32 is used for the synthesis of the Lyapunov based predictive controller of Eqs.4.19–4.24 which is the implemented on a 30th order Galerkin discretization on the parabolic PDE system (higher order discretization led to identical results).

For stabilizing the process at the nominal equilibrium distribution, the Lyapunov based MPC of Section 4.3.1 is designed using a quadratic Lyapunov function of the form $V = x^T P x$ with $P = \begin{bmatrix} 73.6050 & 53.6864 \\ 53.6864 & 45.3090 \end{bmatrix}$, where the matrix P is computed by solving the Riccati inequality with the linearized system matrices. The parameters in the objective function of Eq.4.24 are chosen as $Q = P$, and $R = rI$, with $r = 0.002$. The stability region

estimate Ω_s for the infinite dimensional system under the Lyapunov-based predictive controller as per Theorem 4.1 is computed and shown in Fig.4.7. The constrained nonlinear optimization problem is solved using the MATLAB function FMINCON, and the set of ODEs is integrated using the MATLAB solver ODE15s. The eigenmode amplitudes for the nominal operating equilibrium distribution corresponding to the nominal values of the manipulated inputs of $u^1 = -0.35$, and $u^2 = -0.45$ are $(a_1(0), a_2(0)) = (0.2213, -0.0651)$. An open–loop simulation is first performed starting at the initial condition $(a_1(0), a_2(0)) = 1.0001(0.2213, -0.0651)$. As can be seen in Fig.4.1, the nominal equilibrium is unstable as the exothermicity of the reaction causes the temperature profile to escape to a higher temperature distribution. This demonstrates the need for feedback control to stabilize the process at this unstable steady-state distribution. We show the implementation of the predictive control algorithm on the initial condition $(a_1(0), a_2(0)) = (0.1, 0.03)$ which is within the estimate of the stability region (see Fig.4.3), with the objective of stabilizing at the nominal unstable distribution. The predictive controller is able to continuously reduce the value of the Lyapunov function, and hence (as can be seen from the temperature profile in Fig.4.2) achieves practical closed–loop stability of the infinite dimensional system and drive the process sufficiently close to the nominal equilibrium distribution. The corresponding phase-plane for the amplitudes of the slow eigenmodes and manipulated input profiles can be seen in Fig.4.3 and Fig.4.4, respectively.

4.4 Safe-parking of transport-reaction processes

Having presented a Lyapunov-based predictive control formulations that allow for the explicit characterization of the stability region under fault-free and faulty conditions, in this section, a framework is presented which in the event of a fault determines a 'safe-parking' distribution where the process can be temporarily operated utilizing the depleted control action and enable resumption of nominal operation upon fault repair.

4.4.1 Methodology

In this section, we use the stability region characterizations of the predictive controller presented in Section 4.3.1 to identify 'safe-parking' distributions so that the switching scheme outlined by this framework guarantees the transition to the 'safe-parking' distribution (with depleted control action), and back to the nominal distribution (with full control action). To account for the presence of constraints on the manipulated inputs, the key requirements for a safe-park distributions include that the process state at the time of the actuator fault resides in the stability region for the safe-park distribution (so the process can be driven to the candidate safe-park distribution), and that the safe-park distribution should reside in the stability region under nominal operation (so the process can be returned to nominal operation). These requirements are formalized in Theorem 4.2 below.

To this end, consider the system of Eq.4.1 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 for the infinite dimensional system under nominal operation, denoted by Ω_s^n, has been characterized for the predictive controller formulation of Eqs.4.19–4.24. Similarly, for a candidate safe-park distribution x_{sp}, we denote Ω_s^{sp} as the stability region (computed *a priori*) of the infinite dimensional system under the predictive controller of Eqs.4.19–4.24. We also denote $u_{2,x_{sp}} = u_{MPC}(\bar{x}_s, x_{sp}, u_{min,2}, u_{max,2})$, as the control law designed to stabilize at the candidate safe-park distribution (using the depleted control action), where $u_{min,2}$, $u_{max,2}$ denote the constraints on the manipulated variables in the presence of a fault.

Theorem 4.2 : *Consider the constrained system of Eq.4.1 under the MPC law of Eqs.4.19–4.24 designed to achieve* $\limsup_{t\to\infty} |x_s(t)| \leq d$ *and* $\limsup_{t\to\infty} \|x_f(t)\|_2 \leq d$ *for a given positive number d. If* $x_s(0) \in \Omega_s^n$, $x_s(T^{fault}) \in \Omega_s^{sp}$ *and* $\Omega_s^{sp} \subset \Omega_s^n$, *then the switching rule*

$$u(t) = \left\{ \begin{array}{lll} u_{1,n} & , & 0 \leq t < T^{fault} \\ u_{2,x_{sp}} & , & T^{fault} \leq t < T^{repair} \\ u_{1,n} & , & T^{repair} \leq t \end{array} \right\} \tag{4.33}$$

guarantees that $x_s(t) \in \Omega_s^n \; \forall \, t \geq 0$ *and infinite-dimensional closed-loop system is practically*

stable in the sense that $\limsup_{t\to\infty} |x_s(t)| \leq d$ *and* $\limsup_{t\to\infty} \|x_f(t)\|_2 \leq d$.

Proof of Theorem 4.2: We consider the two possible cases; first if no fault occurs ($T^{fault} = T^{repair} = \infty$), and second if a fault occurs at a time $T^{fault} < \infty$ and is repaired at a time $T^{fault} \leq T^{repair} < \infty$.

Case 1: The absence of a fault implies $u(t) = u_{1,n}\ \forall\ t \geq 0$. Since $x_s(0) \in \Omega_s^n$, and the nominal control configuration is implemented for all times, we have from Theorem 4.1 that $x_s(t) \in \Omega_s^n\ \forall\ t \geq 0$ and $\limsup_{t\to\infty} |x_s(t)| \leq d$, $\limsup_{t\to\infty} \|x_f(t)\|_2 \leq d$.

Case 2: At time T^{fault}, the control law designed to stabilize the process at x_{sp} is activated and implemented till T^{repair}. Since $x_s(T^{fault}) \in \Omega_s^{sp} \subset \Omega_s^n$, we have that $x_s(t) \in \Omega_s^n\ \forall\ T^{fault} \leq t \leq T^{repair}$. At a time T^{repair}, we therefore also have that $x_s(T^{repair}) \in \Omega_s^n$. Subsequently, as with case 1, the nominal control configuration is implemented for all time thereafter, we have that $x_s(t) \in \Omega_s^n\ \forall\ t \geq T^{repair}$. In conclusion, we have that $x_s(t) \in \Omega_s^n\ \forall\ t \geq 0$ and $\limsup_{t\to\infty} \|x_s(t)\| \leq d$. This completes the proof of Theorem 4.2. □

Remark 4.7: Note that the entire design of the safe-parking candidates is carried out off-line, and only the decision as to a particular choice of a safe-park point is made online, upon fault occurrence. In particular, for a fail-safe position of an actuator, the entire set of candidate safe-park points X_{sp} can be computed off-line. In addition the corresponding stability (and invariant) regions subject to depleted control action can also be computed off-line (as is done for the nominal equilibrium distribution). Note as per Theorem 4.1, all stability regions are characterized using the slow-states x_s, while Theorem 4.2 outlines the criteria for selecting the safe-park distributions. Specifically, the Theorem requires that the stability (and invariant) region of the candidate safe-park distribution be such that the slow state at the time of the failure resides in the stability region for the safe-park distribution. This ensures that the process can be driven to the safe-park distribution with the remaining depleted control action. Furthermore, the theorem requires that the stability (and invariant) region for a safe-park distribution be completely contained in the stability region under nominal operation. This ensures that the slow-state trajectory always stays within the

stability region under nominal operation, thereby enabling smooth transition to nominal operation upon fault recovery (see [36] for a discussion on relaxing this requirement).

Remark 4.8: Referring to the practical implementation of the result in Theorem 4.2, one must initially determine the set of candidate safe-park distributions. Note that although the computation of the control law developed in Section 4.3.1 which is used within the safe-parking framework neglects the evolution of the fast states, the computation of the candidate safe-park distributions uses both the slow and fast states. Specifically, using a suitable Galerkin discretization of the parabolic PDE system, the equilibrium states of the approximate ODEs which correspond to the failed actuator at fail-safe position, and the other manipulated inputs at admissible values, must be solved. These equilibrium states correspond to equilibrium distributions for the PDE system and are the candidate safe-park distributions. A suitable Lyapunov function is then used to construct estimates of the stability region for each possible fault scenarios for a given set of manipulated inputs. The switching logic outlined in Theorem 4.2 is then checked on-line to determine, for a given fault, suitable safe-park distributions.

Remark 4.9: The proposed safe-parking framework is different than previously developed safe-parking schemes in that the present work considers infinite-dimensional systems modeled by dissipative quasi-linear PDEs. The frameworks in [36] and chapter 3 were developed for spatially homogeneous processes which could be modeled by ODEs. By considering lumped parameter systems the frameworks in [36] and chapter 3, work with safe-park points, where the process could be temporarily preserved upon a fault. In contrast, this chapter considers processes with spatial variation and thus the framework stabilizes the process at steady–state spatial distributions rather than points. Furthermore, the construction of the stability region estimates must account for the infinite dimensional nature of the system. This is done by using the time scale separation of the eigenspectrum to construct an estimate for the reduced order system, and then making this estimate slightly more conservative to compensate for the remaining neglected eigenmodes. Subsequently, the safe-parking decisions are implemented based on the slow states residing within the conservative stability region estimate.

Remark 4.10: The assumption of actuators reverting to fail-safe positions upon failure is common practice for actuators which have a fail-safe mechanism. The fail-safe positions are chosen to minimize the possibility of hazardous conditions, e.g. high temperatures and pressures. For example, the fail-safe position of a coolant valve and steam valve would be the fully open and fully closed position respectively. This assumption allows for the *a priori* enumeration of the possible fault scenarios for a given set of manipulated inputs. For each possible fault scenario, the safe-park candidates, and appropriate safe-park distributions can be determined. Note that the safe-park distribution is chosen online (the condition $x_s \in \Omega_s^n$ can be verified off-line, however $x_s(T^{fault}) \in \Omega_s^{sp}$ has to be verified online, upon fault-occurrence) and can be done via simply evaluating the Lyapunov function. Note also that while the proposed safe-parking framework assumes *a priori* knowledge of the fail-safe positions of the actuators, it does not require *a priori* knowledge of the fault and repair times, and only provides appropriate switching logic that is executed when, and if, a fault takes place and is subsequently rectified.

Remark 4.11: The safe-parking framework as outlined in Theorem 4.2 addresses the problem where a fault occurs that precludes operation at nominal operating distribution, and provides an appropriately characterized safe-park distribution where the process can be temporarily held until nominal operation can be resumed. Note that the safe-parking framework addresses a problem not considered by the reconfiguration-based approaches of [29; 30; 19]. In particular, we consider faults for which the nominal equilibrium point is no longer an equilibrium point, and we address the case where no backup control configuration is available (for which the nominal equilibrium point continues to be an equilibrium point). Note also, that the criteria for choosing safe-park distributions may lead to several safe-park candidates being suitable. The choice can then be made by incorporating optimality considerations in the safe-parking framework. Specifically, having determined the appropriate safe-park distributions, the cost of transitioning to the safe-park distribution, the cost of operating at the safe-park distribution, as well as resuming nominal operation can be estimated using an auxiliary controller (see [36] for the incorporation of performance considerations in the safe-parking framework for lumped-parameter systems).

4.4.2 Safe-parking of the diffusion-reaction process

In this section, we demonstrate the implementation of the proposed safe-parking mechanism from Section 4.4.1 to the diffusion-reaction process of Eqs.4.13-4.14. We use the same model representation in terms of evolution of the amplitudes of the eigenmodes as in Section 4.3.2.

To this end, consider the scenario where the process is stabilized at the nominal operating distribution. At $t = 0.5\ min$, a fault occurs in the coolant flow rate (centered around the point $z = \pi/3$), and reverts to the fail-safe position (fully open). Hence only one actuator at $z = 2\pi/3$ is functioning, and the nominal steady–state operating distribution corresponding to $u^1 = -0.35$, and $u^2 = -0.45$ is no longer an equilibrium distribution of the process subject to the fault in u^1. To demonstrate the need for implementing the safe-parking approach, we first show a possible outcome if the controller simply tries to preserve nominal operation using the functioning actuator. Attempting to continue operating at this nominal distribution using the proposed predictive controller results in the process escaping to an undesired stable equilibrium which corresponds to a very high temperature (as can be seen from the temperature profile in Fig.4.5). The corresponding state and input trajectory are shown by dashed lines in Fig.4.7 and Fig.4.8 respectively. Specifically, as the coolant flow centered at $z = \pi/3$ reverts to the fully open position, the remaining functioning actuator at $z = 2\pi/3$ must begin to counter the affect of the cooling in order to maintain the process at the nominal operating temperature profile. This decrease is immediately followed by an increase in the coolant for the functioning actuator as the exothermicity of the reaction accelerates the increase in temperature. Since no admissible value of the functioning actuator will result in the nominal operating distribution to be a steady–state distribution, the functioning actuator eventually saturates at the fully open position in attempt to counter the exothermicity of the reaction. However, this cooling is inadequate to counter the exothermicity of the reaction and results in the state profile escaping to a high temperature steady–state distribution. In contrast, if the fault is handled using the proposed safe-parking mechanism, a safe-park distribution corresponding to slow amplitudes of the eigenmodes of $(a_1(0), a_2(0)) = (0.1, 0.03)$ is chosen. This safe-park distribution is contained within the stability region of the nominal operating distribution, and the nominal operating

distribution is also contained within the stability region for this safe-park distribution. Thus this safe-park distribution meets the criteria outlined in Theorem 4.2. The stability region estimates for the nominal (dashed–dotted line) and safe parking distributions (dotted line) can be seen Fig.4.7, and are denoted by Ω_s^n and Ω_s^{sp} respectively. The process is driven to, and stabilized at the safe-parking point using the remaining functioning point actuator at $z = 2\pi/3$. Since at the time of the fault, the process is within the stability region of the safe-park distribution, successful stabilization at the safe-park distribution is ensured (Theorem 4.2). At $t = 4.6$ minutes the fault is rectified. The safe-parking mechanism reverts the controllers to use both functioning actuators and is able to drive the process back to the original nominal equilibrium point. This successful stabilization is ensured (again by Theorem 4.2), since at the time of fault recovery, the process was within the stability region of the nominal operating distribution. The state trajectory under the safe-parking mechanism is shown in Fig.4.7 (solid lines). The temperature profile during the fault and fault recovery stages, under the safe-parking framework can be in Fig.4.6. The corresponding manipulated input profiles can be seen in Fig.4.8 with solid lines.

4.5 Conclusions

This chapter considered the problem of model predictive control and handling actuator faults in transport-reaction processes subject to input constraints. First, a Lyapunov-based model predictive controller was designed which establishes closed–loop practical stability of the infinite dimensional system, while simultaneously providing an explicitly characterized stability region. This predictive control formulation was then used to develop a framework to handle faults that preclude the possibility of continued operating at the nominal equilibrium distribution using robust or reconfiguration-based fault-tolerant control approaches. This framework utilizes pre–specified (candidate safe-park) distributions where the process can be temporarily maintained. Such distributions are chosen to prevent the onset of hazardous situations as well ensure smooth resumption of nominal operation upon fault-repair. Specifically, a safe-parking distribution is chosen based on the following criteria: 1) the pro-

cess state at the time of failure resides in the stability region of the safe-park distribution (subject to depleted control action), and 2) the safe-park distribution resides within the stability region of the nominal control configuration. The proposed framework was illustrated using a diffusion–reaction process.

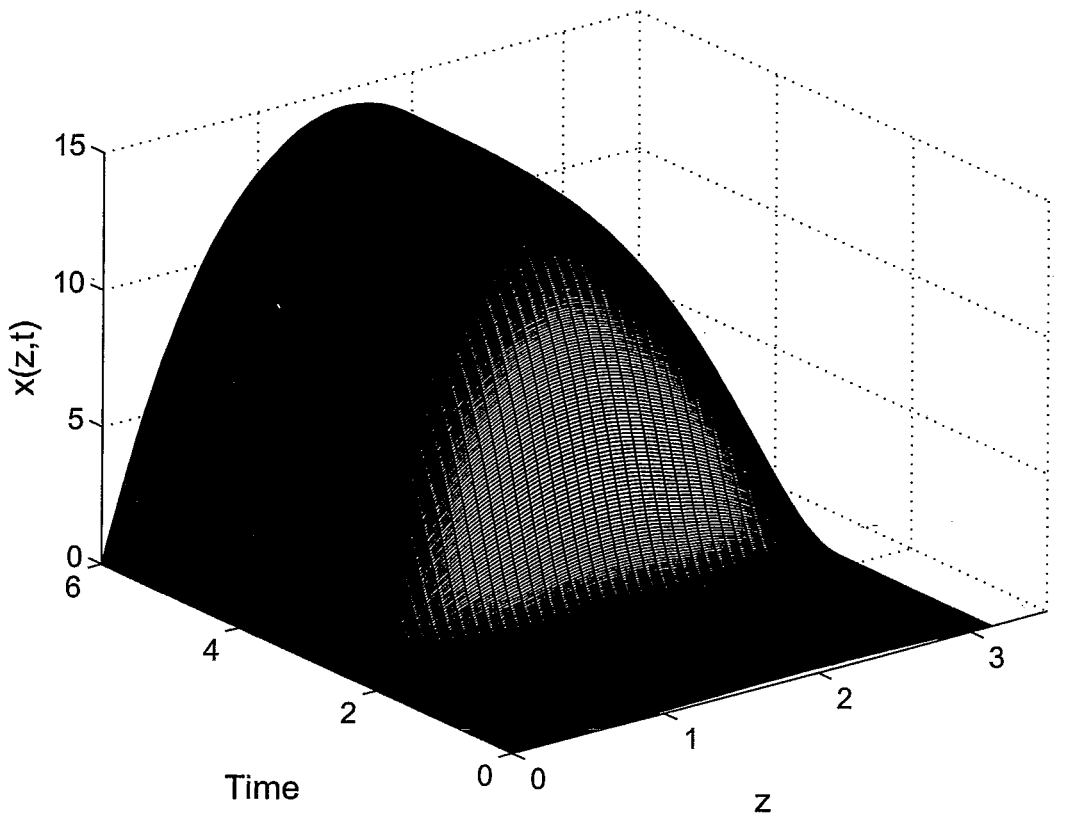

Figure 4.1: Open–loop dimensionless temperature profile for the diffusion-reaction process.

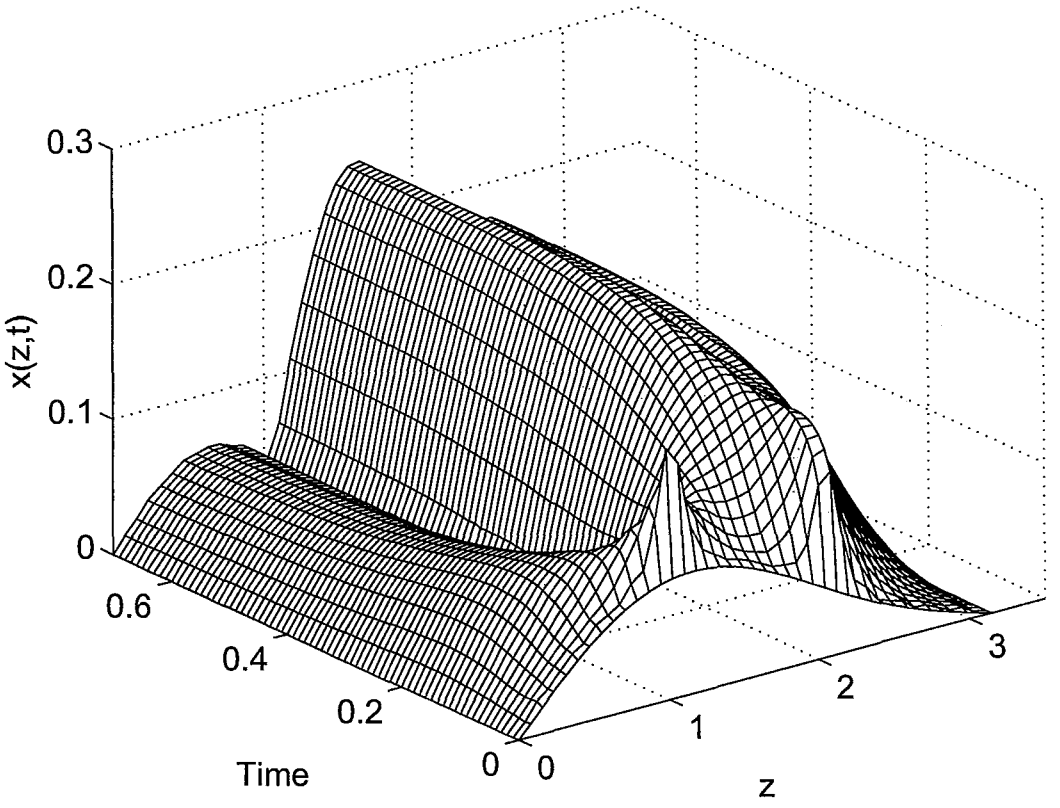

Figure 4.2: Closed–loop dimensionless temperature profile under the implementation of the proposed predictive controller with $(a_1(0), a_2(0)) = (0.1, 0.03)$.

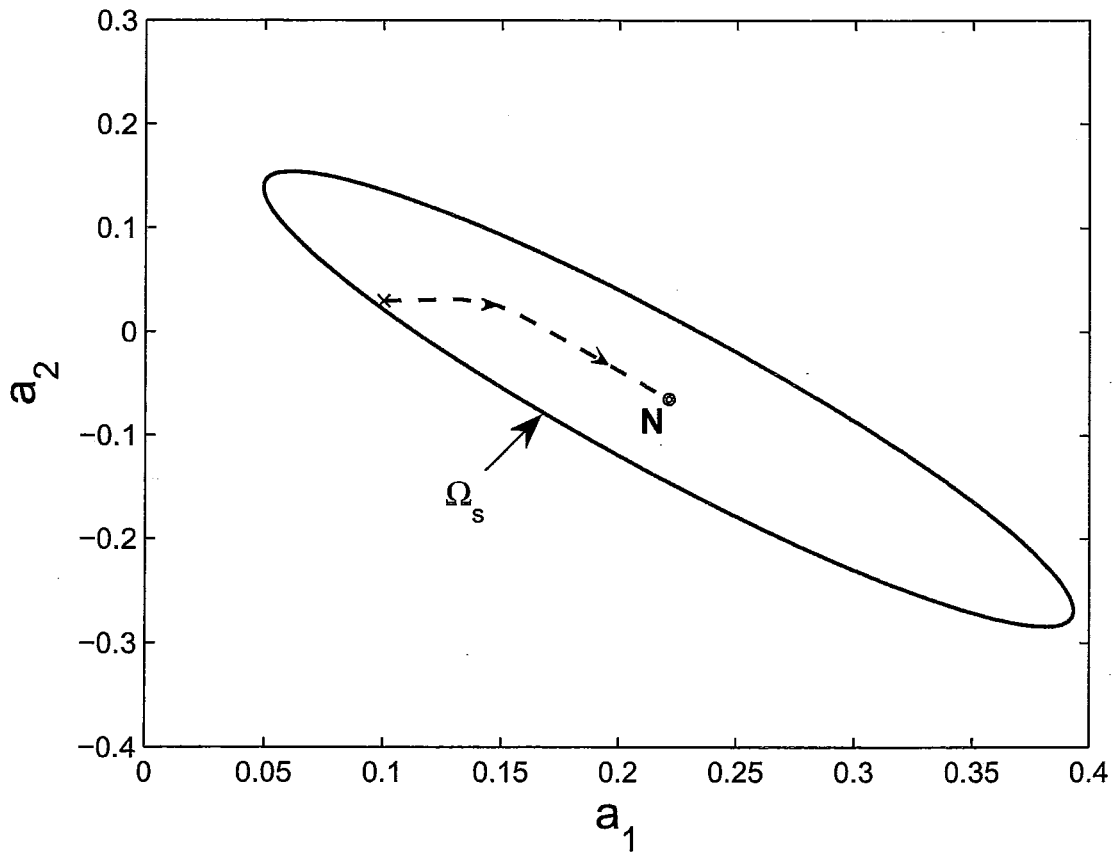

Figure 4.3: Dashed line (- -) indicates the evolution of the state trajectory for slow states, and Ω_s denotes the stability region estimate under the proposed predictive control formulation.

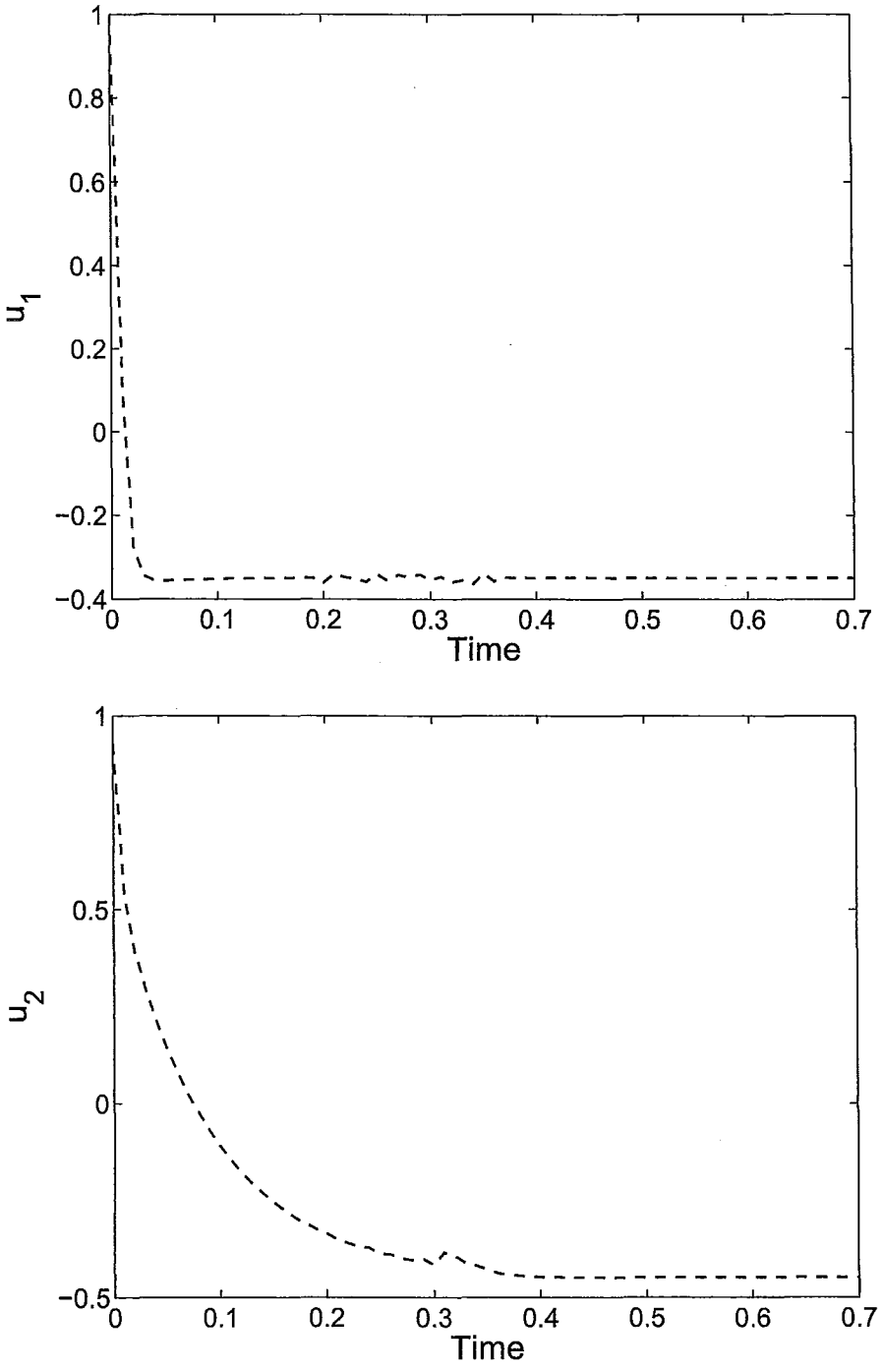

Figure 4.4: Manipulated input profiles under the implementation of the proposed predictive controller with $(a_1(0), a_2(0)) = (0.1, 0.03)$.

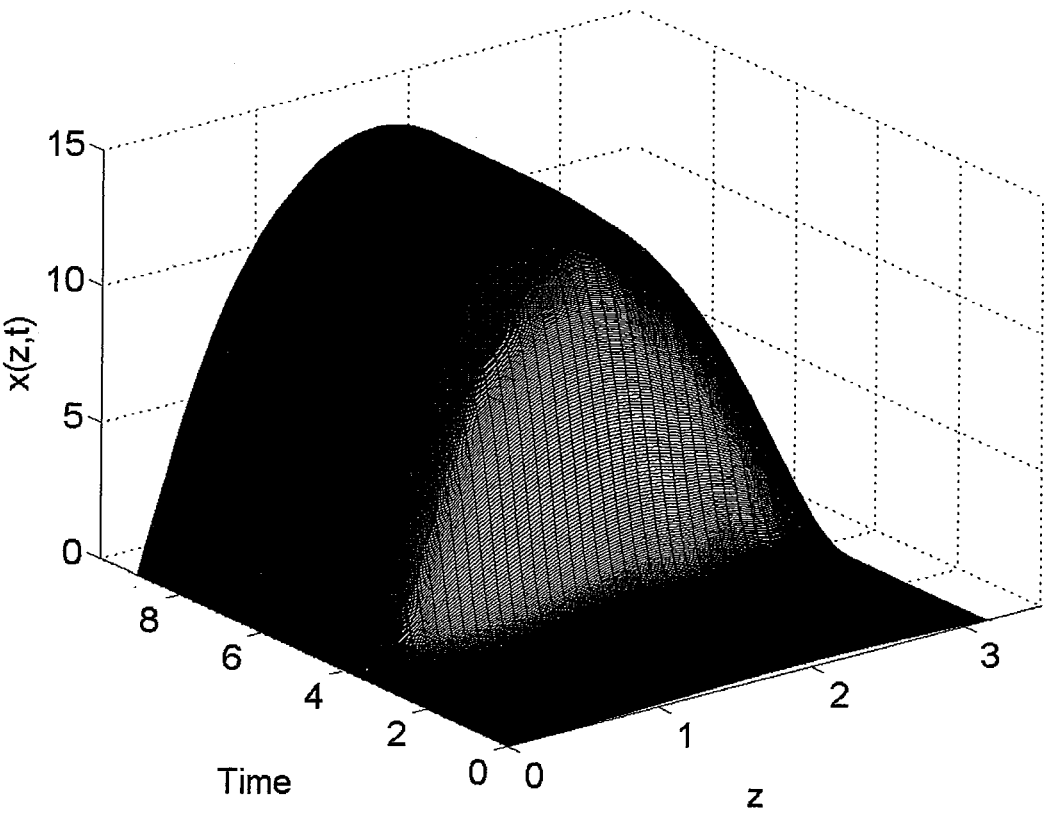

Figure 4.5: Closed–loop dimensionless temperature profile in the presence of actuator faults. At $t = 0.5$ *min* a fault occurs to the point actuator at $z = \pi/3$, and this actuator reverts to the fully open position. Continued operation at the nominal equilibrium is attempted and is not achievable. The process escapes to a potentially hazardous high temperature distribution.

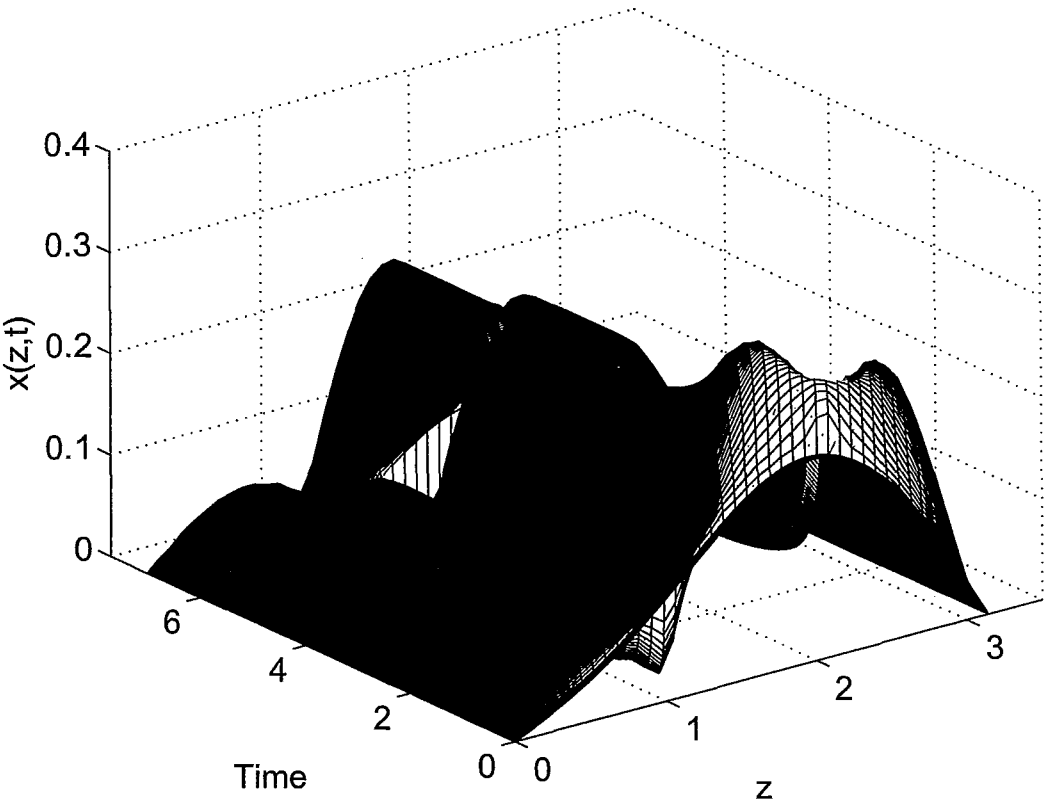

Figure 4.6: Closed–loop dimensionless temperature profile in the presence of actuator faults under the implementation of the safe-park mechanism. At $t = 0.5$ *min* a fault occurs to the point actuator at $z = \pi/3$, and this actuator reverts to the fully open position. With the remaining functioning actuator at $z = 2\pi/3$, the process is stabilized at a safe-park point. Upon fault recovery at $t = 4.6$ *min*, the process is successfully driven back to nominal operation using both point actuators.

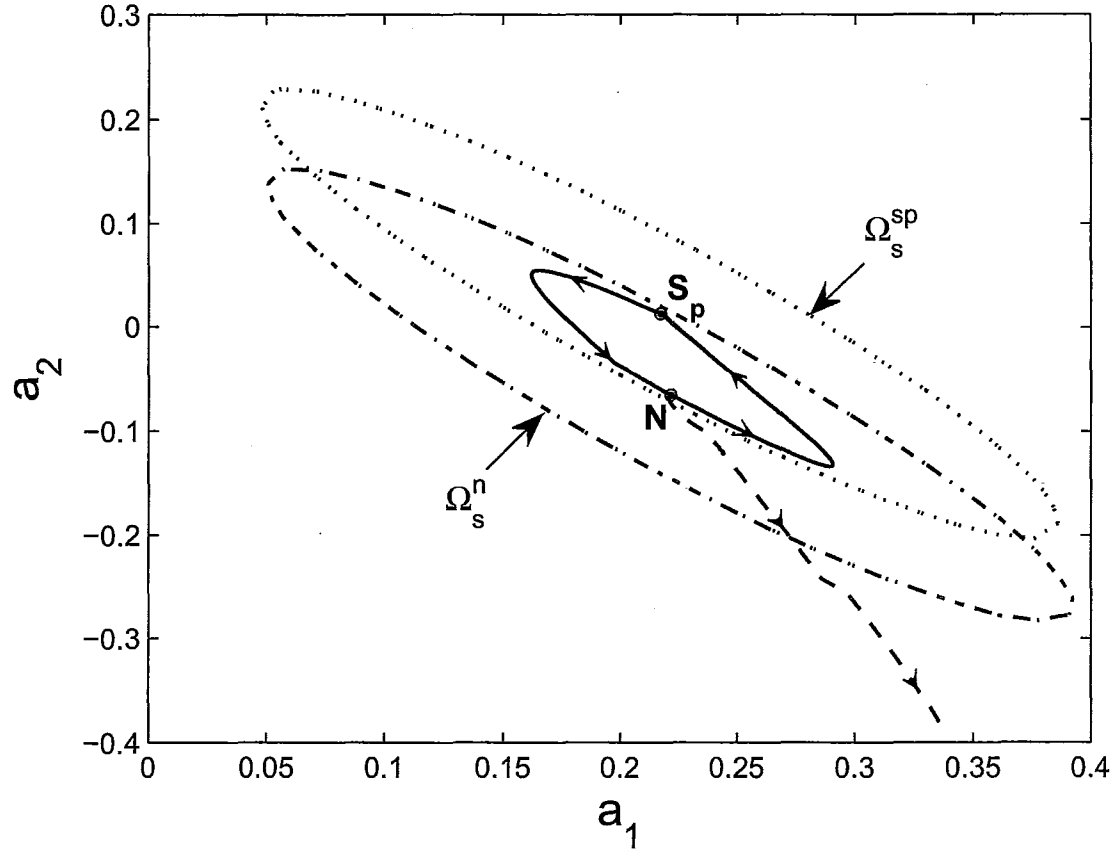

Figure 4.7: Evolution of the state trajectory for slow states in the presence of actuator faults. Dashed line (- -) indicates the case when a continued operation at the nominal operating condition in the presence of a fault is attempted. Solid line (–) indicates the case when the process is stabilized at the safe park distribution S_p which is chosen according to Theorem 2. This guarantees resumption of nominal operation upon fault-recovery. Ω_s^n and Ω_s^{sp} (dashed–dotted line (-.-), and dotted line (.)), denote the nominal and safe-parking distribution stability region estimates respectively.

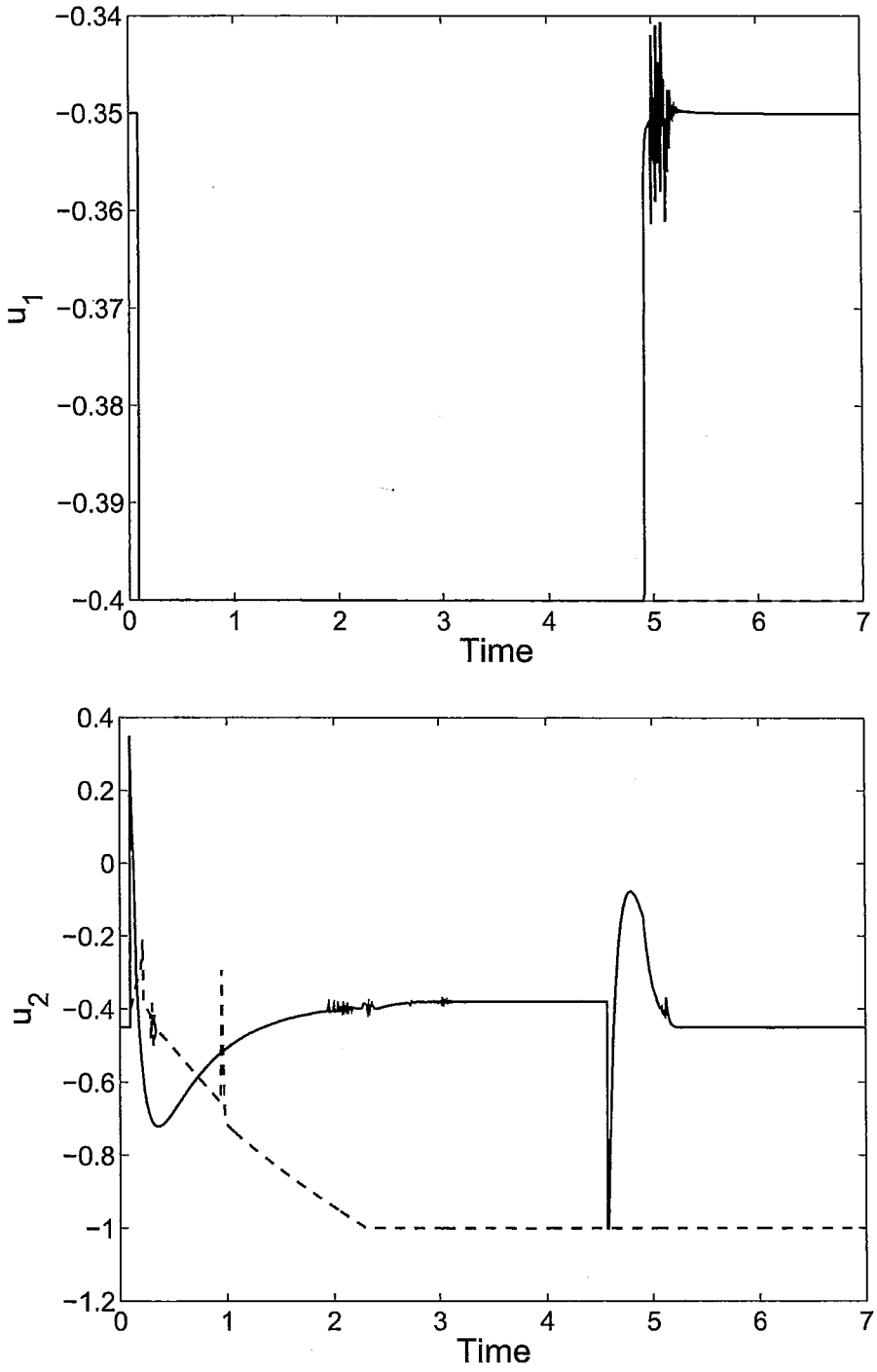

Figure 4.8: Manipulated input profiles in the presence of actuator faults. Fault occurs at 0.1 *min* and is rectified at 4.6 *min*. The dashed lines (- -) represent trying to continue operation at the nominal operation conditions using the depleted control action. The solid lines (—) represent operation under the proposed safe-parking mechanism.

Chapter 5

Conclusions and Recommendations

5.1 Conclusions

This thesis considered the design and applications of predictive control of nonlinear process systems subject to input constraints. In chapter 2, continuous-time nonlinear process systems were considered, and a predictive control formulation was presented which enhances the set of initial conditions from where closed-loop stability can be achieved. The main idea in this formulation was to employ characterization of the process dynamics which were independent of the specific control-law used. Linear process systems were first considered as a subcase. For linear systems a predictive controller was designed that achieves closedloop stability for every initial condition in the null controllable region. For nonlinear process systems, suitable constraints are formulated within the predictive controller which require the process to remain within the region where a given Lyapunov function value can be made to decay. The incorporation of this constraint expanded on the set of initial conditions from where closedloop stability can be achieved, and thus better utilized the constraint handling capabilities of MPC. The proposed method was illustrated using a chemical reactor example, and the robustness with respect to parametric uncertainty and disturbances demonstrated via application to a styrene polymerization process. In chapter 3, this predictive control design was further broadened by considering the presence of uncertainty and lack of full

state measurements. The problem of fault handling was also given attention. Specifically, a safe-parking scheme was developed for actuator faults which preclude the possibility of continued nominal operation using the existing robust or reconfiguration-based fault-tolerant control approaches. Using the proposed robust/output feedback control design, the scheme extended a previously developed safe-parking framework to handle uncertainty and lack of full state measurements. The proposed framework was illustrated using a chemical reactor example and demonstrated on a styrene polymerization process. Finally in chapter 4, we considered transport-reaction processes described by quasi-linear PDEs subject to input constraints. A Lyapunov-based model predictive controller which provides an explicit characterization of the set of initial conditions from where closed-loop stability of the parabolic PDE system is guaranteed was first developed. This was done by deriving a finite set of ODEs which capture the dominant dynamics of the infinite-dimensional system via Galerkins method. Similar to the continuous-time setting, this control design was then subsequently used to develop a safe-parking framework for handling actuator faults. Safe-parking for distributed parameter systems is intuitively similar to continuous-time systems, with equilibrium distributions replacing equilibrium points. Utilizing the stability region characterization provided by the developed predictive controller, safe-park distributions from the safe-park candidates (equilibrium distributions subject to failed actuators) are chosen to preserve closed-loop stability upon fault repair. The proposed framework was illustrated on a diffusion-reaction process.

5.2 Recommendations for Further Work

One interesting avenue to explore is the reformulation of the predictive control design in chapter 2 for linear systems within a Lyapunov framework. The presented design utilized the description of the boundary of the null-controllable region as level sets of an energy-like function. Decay of the function was enforced via constraints in the MPC design, and the feasibility and stability guarantees were shown for all initial conditions within the null-controllable region. However, this analysis and design did make use of any Lyapunov-based

tools. The ability to characterize the null-controllable region within a Lyapunov framework would be of great value. Specifically, it would provide a systematic procedure to construct control Lyapunov functions for linear systems which accounts for the presence of input constraints. In light of the fact that the construction of Lyapunov functions remains to be a bottleneck of all Lyapunov-based control designs, this construction procedure would be very beneficial.

Furthermore, another interesting avenue to explore is the extension of the stabilizing control design presented for linear systems in chapter 2 to the nonlinear platform. Although characterizations of the exact null-controllable region are in general not available for nonlinear systems, one approach could be to design a similar control scheme using some sort of maximal estimates of the region.

There are several directions for the further development of the fault-tolerant safe-parking scheme. Namely, the extension to multi-unit processes which involve recycle streams, the incorporation of sensor failures, and the integration with switched control schemes. In addition, given that many chemical processes involve distributed variables which are modelled by PDEs, the safe-parking framework for transport-reaction processes presented in chapter 4 can be extended to other PDE systems (e.g. hyperbolic).

List of References

[1] F. Allgower and H. Chen. Nonlinear model predictive control schemes with guaranteed stability. In R. Berber and C. Kravaris (Eds.), *NATO ASI on Nonlinear Model Based Process Control*, pages 465–494, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1998.

[2] H. B. Aradhye, B. R. Bakshi, J. F. Davis, and S. C. Ahalt. Clustering in wavelet domain: A multiresolution art network for anomaly detection. *AIChE J.*, 50:2455–2466, 2004.

[3] A. Armaou and P. D. Christofides. Wave suppression by nonlinear finite-dimensional control. *Chem. Eng. Sci.*, 55:2627–2640, 2000.

[4] A. Armaou and M. A. Demetriou. Robust detection and accommodation of incipient component and actuator faults in nonlinear distributed processes. *AIChE J.*, 54:2651–2662, 2008.

[5] A. Armou and P. D. Christofides. Dynamic optimization of dissipative PDE systems using nonlinear order reduction. *Chem. Eng. Sci.*, 57:5083–5114, 2002.

[6] Ding B and B. Huang. Constrained robust model predictive control for time-delay systems with polytopic description. *Int. J. Contr.*, 80:509–522, 2007.

[7] Ding B and B. Huang. Output feedback model predictive control for nonlinear systems represented by hammerstein-wiener model. *IET Contr. Th. App.*, 1:1302–1310, 2007.

[8] J. Baker and P. D. Christofides. Finite dimensional approximation and control of nonlinear parabolic PDE systems. *Int. J. Contr.*, 73:439–456, 2000.

[9] M. J. Balas. Feedback control of linear diffusion processes. *Int. J. Contr.*, 29:523–533, 1979.

[10] W. B. Bequette. Nonlinear control of chemical processes: A review. *Ind. & Eng. Chem. Res.*, 30:1391–1413, 1991.

[11] G. Bitsoris and M. Vassilaki. Constrained regulation of linear systems. *Automatica*, 31:223–227, 1995.

[12] D. Chmielewski and V. Manousiouthakis. On constrained infinite-time linear quadratic optimal control. *Syst. Contr. &. Lett.*, 29:121–129, 1996.

[13] P. D. Christofides. *Nonlinear and Robust Control of PDE Systems: Methods and Applications to Transport-Reaction Processes,*. Birkhäuser, Boston, 2000.

[14] P. D. Christofides and P. Daoutidis. Finite-dimensional control of parabolic PDE systems using approximate inertial manifolds. *J. Math. Anal. Appl.*, 216:398–420, 1997.

[15] P. D. Christofides, J. F. Davis, N. H. Farra, D. Clark, K. R. D. Harris, and J N. Gibson Jr. Smart plant operations: Vision, progress and challenges. *AIChE J.*, 53:2734–2741, 2007.

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

[17] P. D. Christofides and A. R. Teel. Singular perturbations and input-to-state stability. *IEEE Trans. Autom. Contr.*, 41:1645–1650, 1996.

[18] J. F. Davis, M. L. Piovoso, K. Kosanovich, and B. Bakshi. Process data analysis and interpretation. *Advances in Chemical Engineering*, 25:1–103, 1999.

[19] M. A. Demetriou, N.H. El-Farra, and P. D. Christofides. Actuator and controller scheduling in nonlinear transport-reaction processes. *Chem. Eng. Sci.*, 63:3537–3550, 2008.

[20] C. DePersis and A. Isidori. A geometric approach to nonlinear fault detection and isolation. *IEEE Trans. Automat. Contr.*, 46:853–865, 2001.

[21] S. Dubljevic and P. D. Christofides. Predictive control of parabolic PDEs with boundary control actuation. *Chem. Eng. Sci.*, 61:6239–6248, 2006.

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

[23] S. Dubljevic, P. Mhaskar, N. H. El-Farra, and P. D. Christofides. Predictive control of transport-reaction processes. *Comp. & Chem. Eng.*, 29:2335–2345, 2005.

[24] S. Dubljevic, P. Mhaskar, N. H. El-Farra, and P. D. Christofides. Predictive control of parabolic PDEs with state and control constraints. *Int. J. Rob. & Non. Contr.*, 16:749–772, 2006.

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

[26] N. H. El-Farra, A. Armou, and P. D. Christofides. Analysis and control of parabolic PDE systems with input constraints. *Automatica*, 39:715–725, 2003.

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

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

[29] N. H. El-Farra and P. D. Christofides. Coordinated feedback and switching for control of spatially distributed processes. *Comput. Chem. Eng. Res.*, 28:111–128, 2004.

[30] N. H. El-Farra and S. Ghantasala. Actuator fault isolation and reconfiguration in transport-reaction processes. *AIChE J.*, 53:1518–1537, 2007.

[31] N. H. El-Farra, P. Mhaskar, and P. D. Christofides. Hybrid predictive control of nonlinear systems: Method and applications to chemical processes. *Int. J. Rob. & Non. Contr.*, 4:199–225, 2004.

[32] N. H. El-Farra, P. Mhaskar, and P. D. Christofides. Output feedback control of switched nonlinear systems using multiple Lyapunov functions. *Sys. & Contr. Lett.*, 54:1163–1182, 2005.

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

[34] P. M. Frank and X. Ding. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *J. Proc. Contr.*, 7:403–424, 1997.

[35] A. Friedman. *Partial Differential Equations.* Holt, Rinehart & Winston, New York, 1976.

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

[37] R. Goebel. Stabilizing a linear system with saturation through optimal control. *IEEE Trans. Automat. Contr.*, 50:650–655, 2005.

[38] P. O. Gutman and M. Cwikel. Admissible-sets and feedback-control for discrete-time linear dynamic-systems with bounded controls and states. *IEEE Trans. Automat. Contr.*, 31:373–376, 1986.

[39] P. M. Hidalgo and C. B. Brosilow. Nonlinear model predictive control of styrene polymerization at unstable equilibrium point. *Comp. & Chem. Eng.*, 14:481–494, 1990.

[40] T. Hu, Z. Lin, and L. Qiu. An explicit description of null controllable regions of linear systems with saturating actuators. *Sys. & Contr. Lett.*, 47:65–78, 2002.

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

[42] N. Kapoor, A. R. Teel, and P. Daoutidis. An anti-windup design for linear systems with input saturation. *Automatica*, 34:559–574, 1998.

[43] N. Kazantzis and C. Kravaris. Nonlinear observer design using Lyapunov's auxiliary theorem. *Syst. & Contr. Lett.*, 34:241–247, 1998.

[44] S. L. D. Kothare and M. Morari. Contractive model predictive control for constrained nonlinear systems. *IEEE Trans. Automat. Contr.*, 45:1053–1071, 2000.

[45] J. V. Kresta, J. F. Macgregor, and T. E. Marlin. Multivariate statistical monitoring of process operating performance. *Can. J. Chem. Eng.*, 69:35–47, 1991.

[46] J. LeMay. Recoverable and reachable zones for control systems with linear plants and bounded controller outputs. *IEEE Trans. Automat. Contr.*, 9:346–354, 1964.

[47] D. Limon, T. Alamo, F. Salas, and E. F. Camacho. On the stability of constrained MPC without terminal constraint. *IEEE Trans. Automat. Contr.*, 51:832–836, 2006.

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

[49] Y. H. Lu, Y. Arkun, and A. Palazoglu. Real-time application of scheduling quasi-min-max model predictive control to a bench-scale neutralization reactor. *Ind. & Eng. Chem. Res.*, 43:2730–2735, 2004.

[50] L. Magni and R. Sepulchre. Stability margins of nonlinear receding-horizon control via inverse optimality. *Sys. & Contrl. Lett.*, 32:241–245, 1997.

[51] M. Mahmood, R. Gandhi, and P. Mhaskar. Safe-parking of nonlinear process systems: Handling uncertainty and unavailability of measurements. *Chem. Eng. Sci.*, 63:5434–5446, 2008.

[52] M. Mahmood and P. Mhaskar. Enhanced stability regions for model predictive control of nonlinear process systems. *AIChE J.*, 54(6):1487–1498, 2008.

[53] M. Massoumnia, G. C. Verghese, and A. S. Wilsky. Failure detection and identification. *IEEE Trans. Automat. Contr.*, 34:316–321, 1989.

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

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

[56] P. Mhaskar. Robust model predictive control design for fault-tolerant control of process systems. *Ind. Eng. Chem. Res.*, 45(25):8565–8574, 2006.

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

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

[59] 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.*, 55(6):650–659, 2006.

[60] P. Mhaskar, A. Gani, N. H. El-Farra, C. McFall, P. D. Christofides, and J. F. Davis. Integrated fault-detection and fault-tolerant control for process systems. *AIChE J.*, 52:2129–2148, 2006.

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

[62] D. Munoz de la Pena and P. D. Christofides. Output feedback control of nonlinear systems subject to sensor data losses. *Syst. & Contr. Lett.*, 57:631–642, 2008.

[63] K. R. Muske and J. B. Rawlings. Model predictive control with linear-models. *AIChE J.*, 39:262–287, 1993.

[64] D Nagrath, V. Prasad, and B. W. Bequette. A model predictive formulation for control of open-loop unstable cascade systems. *Chem. Eng. Sci.*, 57:365–378, 2002.

[65] A. Negiz and A. Cinar. Statistical monitoring of multivariable dynamic processes with state-space models. *AIChE J.*, 43:2002–2020, 1997.

[66] P. Nomikos and J. F. Macgregor. Monitoring batch processes using multiway principal component analysis. *AIChE J.*, 40:1361–1375, 1994.

[67] N. M. C. Oliveira and L. T. Biegler. Constraint handling and stability properties of model-predictive control. *AIChE J.*, 40:1138–1150, 1994.

[68] P. Pisu, A. Serrani, S. You, and L. Jalics. Adaptive threshold based diagnostics for steer-by-wire systems. *J. Dyn. Sys. Meas. Con.- Trans. ASME*, 128:428–435, 2006.

[69] V. Prasad, M. Schley, L. P. Russo, and B. W. Bequette. Product property and production rate control of styrene polymerization. *J. Proc. Contr.*, 12:353–372, 2002.

[70] J. A. Primbs, V. Nevistic, and J. C. Doyle. A receding horizon generalization of pointwise min-norm controllers. *IEEE Trans. Automat. Contr.*, 45:898–909, 2000.

[71] W. H. Ray. *Advanced Process Control.* McGraw-Hill, New York, 1981.

[72] D. R. Rollins and J. F. Davis. An unbiased estimation technique when gross errors exist in process measurements. *AIChE J.*, 38:563–572, 1992.

[73] J. A. Rossiter, B. Kouvaritakis, and M. Cannon. Computationally efficient algorithms for constraint handling with guaranteed stability and near optimality. *Int. J. Contr.*, 74:1678–1689, 2001.

[74] A. Saberi, A. A. Stoorvogel, P. Sannuti, and H. Niemann. Fundamental problems in fault detection and identification. *Int. J. Rob. & Non. Contr.*, 10:1209–1236, 2000.

[75] P. O. M. Scokaert, D. Q. Mayne, and J. B. Rawlings. Suboptimal model predictive control (feasibility implies stability). *IEEE Trans. Auto. Cont.*, 44:648–654, 1999.

[76] P. O. M. Scokaert and J. B. Rawlings. Feasibility issues in linear model predictive control. *AIChE J.*, 45:1649–1259, 1999.

[77] P. B. Sistu and B. W. Bequette. Nonlinear model-predictive control: Closed-loop stability analysis. *AIChE J.*, 42:3388–3402, 1996.

[78] J. Stephan, M. Bodson, and J. Lehoczky. Calculation of recoverable sets for systems with input and state constraints. *Opt. Contr. Appl. & Meth.*, 19:247–269, 1998.

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

[80] S. Valluri, M. Soroush, and M. Nikravesh. Shortest-prediction-horizon non-linear model-predictive control. *Chem. Eng. Sci.*, 53:273–292, 1998.

[81] Z. Y. Wan and M. V. Kothare. An efficient off-line formulation of robust model predictive control using linear matrix inequalities. *Automatica*, 39:837–846, 2003.

[82] Z. Y. Wan and M. V. Kothare. Efficient scheduled stabilizing model predictive control for constrained nonlinear systems. *Int. J. Rob. & Non. Contr.*, 13:331–346, 2003.

[83] Z. Y. Wan and M. V. Kothare. Efficient scheduled stabilizing output feedback model predictive control for constrained nonlinear systems. *IEEE Trans. Automat. Contr.*, 49:1172–1177, 2004.

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

[85] A Zheng. Stability of model predictive control with time-varying weights. *Comp. & Chem. Eng.*, 21:1389–1393, 1997.