A safe-parking framework to handle faults in nonlinear process systems

Blank Page

A SAFE-PARKING FRAMEWORK TO HANDLE FAULTS IN NONLINEAR PROCESS SYSTEMS

BY

RAHUL GANDHI, M.Tech, (Chemical Engineering)

Indian Institute of Technology-Bombay, India

A THESIS

SUBMITTED TO THE DEPARTMENT OF CHEMICAL ENGINEERING

AND THE SCHOOL OF GRADUATE STUDIES

OF MCMASTER UNIVERSITY

IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

Blank Page

Doctor of Philosophy (2010) McMaster University

(Chemical Engineering) Hamilton, Ontario, Canada

TITLE:	A safe-parking framework to handle faults in nonlinear process systems
AUTHOR:	Rahul Gandhi M.Tech, (Chemical Engineering) Indian Institute of Technology-Bombay, India
SUPERVISOR:	Dr. Prashant Mhaskar
NUMBER OF PAGES:	xxx, 181

Blank Page

This thesis is dedicated to all my friends at Woodlands apartments.

Blank Page

Abstract

This thesis considers the problem of control of nonlinear process systems subject to input constraints and faults in the control actuators and process equipments. Faults are considered that preclude the possibility of continued operating at the nominal equilibrium point and a framework (which we call the safe-parking framework) is developed to enable efficient resumption of nominal operation upon fault-recovery. First, Lyapunov-based model predictive controllers, that allow for an explicit characterization of the stability region subject to constraints on the manipulated input, are designed. The stability region characterization is utilized in selecting 'safe-park' points from the safe-park candidates (equilibrium points subject to failed actuators). This safe-park point is chosen as a temporary operating point where process is to be operated during fault rectification. This ensures that process can be safely operated during fault rectification and the nominal operation can be resumed upon fault recovery. When multiple candidate safe-park points are available, performance considerations, such as ease of transition from and to the safe-park point and cost of running the process at the safe-park point, are quantified and utilized in choosing the optimal safe-park point.

Next, we extend the safe-parking framework to handle practical issues such as

plant-model mismatch, disturbances and unavailability of all process state measurements. We first consider the presence of constraints and uncertainty and develop a robust Lyapunov-based model predictive controller. This controller is utilized to characterize robust stability region which, subsequently, is utilized to select 'safe-park' points. Then we consider the problem of availability of limited measurements. An output feedback Lyapunov-based model predictive controller, with high-gain observer to estimate 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.

We then further extend the framework to handle faults in large scale chemical plants where multiple process units are connected via material, energy and information streams. In plant-wide setting, the safe-park point for the faulty unit is chosen such that the safe-parking has no or minimum effect on downstream units, and hence, the nominal operation in the downstream units can be continued. Next we consider the scenario where no viable safe-park point for the faulty unit exists such that its effect can be completely absorbed in the subsequent unit. A methodology is developed that allows simultaneous safe-parking of the consecutive units. The efficacy of the proposed framework is illustrated using a chemical reactor example, a styrene polymerization process and two CSTRs in series example.

Finally, we demonstrate the efficacy of proposed Lyapunov based Model Predictive Controller and Safe-Parking framework on a polymerization reactor model to control the polymerization reactor and to handle faults that dont allow continuation of the nominal operation in the reactor.

Acknowledgments

I am very much thankful to my supervisor Dr. Prashant Mhaskar for his guidance and support throughout my doctoral research work. His constant motivation and unwavering support encouraged me to thrive during tough times. I have learned lot from him and his "always be cool" attitude has taken lot of pressure off me during tough times.

I would also like to thank my family whose unqualified love and support has helped me travel this journey of PhD smoothly. I thank my beloved Chinar for her unflagging love and support over last couple of years. In addition, I also acknowledge Siam and Zhiwen for the invaluable discussions, which has helped me understand and solve some of challenges I faced. I thank all my friends in Chemical Engineering department and McMaster University. I would like to thank my friends and their families at Woodlands apartments for providing me social support and making my stay at Hamilton memorable.

I also give many thanks to the following professors for the comments they have provided me during my doctoral studies: Chris Swartz, Shahin Sirouspour, Tom Marlin, Benoit Chachuat. Thanks to the administrative staff, Lynn Falkiner, Nanci Cole, Andrea Vickers and Kathy Goodram for their assistance and support over the years.

I would like to thank McMaster Advanced Control Consortium (MACC) and Department of Chemical Engineering at McMaster University for providing financial support and to make my graduate studies possible.

Finally, I must thank almighty god without whose consent nothing is possible.

Contents

List of Figures

List of Tables

Blank Page

List of Symbols

Latin Letters

C_A	Concentrations of A in reactor	kmol/m^3
C_I	Concentrations of the initiator in reactor	kmol/m^3
C_M	Concentrations of the monomer in reactor	kmol/m^3
C_{If}	Inlet concentrations of the initiator stream	kmol/m^3
C_{Mf}	Inlet concentrations of the monomer stream	kmol/m^3
F_c	Coolant flowrate	L/s
F_m	Monomer flowrate	L/s
$J(x;t;u(\cdot))$	Performance index for Model Predictive Controller	
J_r	Cost associated with resuming nominal operation	
J_s	Cost associated with operating at the safe-park point	
J_{tr}	Cost associated with transitioning to the safe-park point	

$k(x)$	Control action calculated by bounded controller	
$L_f V(x)$	Lie Derivative of a scalar function V(x) with respect to vector function f(x)	
P	Matrix in quadratic Lyapunov function, $V = x^T P x$	
Q	Heat added or removed from reactor	kJ/s
Q_w	Positive semi-definite symmetric weighting matrix for process states	
R_w	Positive semi-definite symmetric weighting matrix for inputs	
T	Prediction horizon for Model Predictive Controller	
T	Temperature in reactor	°K
t	Time	min or hr
T^{fault}	Time when fault occurs	min or hr
$T^{recovery}$	Time when fault is repaired	min or hr
T_R	Temperature in reactor	°K
T_{cf}	Inlet temperature of coolant stream	°K
T_c	Temperature in coolant jacket	°K
T_f	Temperature of the inlet stream	°K

T_r	Time required to return to a sufficiently close neighborhood of the nominal operating point starting from safe-park point after fault recovery	min or hr
T_s	Time required to go to a sufficiently close neighborhood of the safe-park point from the nominal operating point in failure scenario	min or hr
$u(t)$	Manipulated variables	
$u_{i,N}(t)$	Control law designed for i^{th} scenario to stabilize process at operating point N	
u_{max}	Maximum value that Manipulated variable can assume	
u_{min}	Minimum value that Manipulated variable can assume	
V	Control Lyapunov function	
V	Volume of reactor	m^3
$x(t)$	Process states	
x_0	States at time, t = 0	
X_c	Set of candidate safe-park points	
x_c	Safe-park point	

Greek Letters

ΔH	Heat of reaction	kJ/kmol
Ω	Stability region for Lyapunov based Model Predictive Controller	
Ω_c	Stability region for safe-park point x_s	
Ω_n	Stability region for nominal operating point N	
Π	State space region where control Lyapunov function can be made to decrease	
ρ	Density	kg/m^3
c_p	Specific Heat	kJ/(kg °C)
E	Activation energy constant in Arrhenius equation	kJ/kmol
R	Gas constant	kJ/(°C kmol)
$'$	Transpose	
θ	Uncertainty in process state evolution	

Superscripts

I	Variables associated with initiator stream
i	i^{th} component of the vector

σ	If $\sigma = 1$ faulty free operation. If $\sigma = 2$ faulty operation
M, m	Variables associated with monomer stream
max	Upper bound on the variable
min	Lower bound on the variable
MPC	Variable associated with Model Predictive Control law
r	Variables associated with resumption of the nominal operation upon fault recovery
s	Variable value at steady state
s	Variables associated with solvent stream
tr	Variables associated transition to the safe-park point on occurrence of fault

Chapter 1

Introduction

Chemical process operation and control involves accounting for process complexity (manifested as nonlinearities), operational issues (such as constraints and disturbances), as well as eventualities, such as faults. Smooth operation of chemical processes, therefore, relies on adequate design and maintenance, appropriate monitoring systems to detect and diagnose eventualities, and the presence of correcting mechanisms that, having been 'informed' of an eventuality, prevent or minimize loss of performance, shutdowns, or hazardous situations. The ubiquitous nature of faults, and the extensive economic damage that results from faults (it is estimated that the U.S. petrochemical industry looses an estimated $20 billion per year due to faults Christofides et al. [2007]) has motivated extensive research on development of strategies for handling faults.

The existing methods for handling faults assume availability of sufficient residual control effort or redundant control configurations to preserve operation at the nominal equilibrium point, and can be categorized within the robust/reliable, and

reconfiguration-based fault-tolerant control approaches. Robust/reliable control approaches (e.g., see Wang et al. [1999]) essentially rely on the robustness of the active control configuration to handle faults as disturbances. Several faults, however, cause significant erosion of the control effort in the active control configuration, and closed-loop stability cannot be preserved by simply re-tuning the controller in the active control configuration. If redundant control configurations are available, control–loop reconfiguration (activating an appropriately chosen fall-back configuration) can be implemented to preserve closed–loop stability at the nominal equilibrium point.

In determining the suitability of a backup control configuration, the presence of constraints, nonlinearity and uncertainty, as well as the switched nature of the closed–loop system (due to the switching between the control configurations) must be accounted for. The extensive research on control of nonlinear and switched systems (see, e.g., Kravaris and Palanki [1988], Lin and Sontag [1991], Bequette [1991], Muske and Rawlings [1993], Valluri and Soroush [1998], Kapoor and Daoutidis [2000], Mayne et al. [2000], Dubljevic and Kazantzis [2002], Mhaskar et al. [2005], Huynh and Kazantzis [2005], Mhaskar et al. [2006a], Christofides and El-Farra [2005]) has made available a number of tools that can be utilized to this end. These include Lyapunov-based nonlinear control designs (see, e.g., Lin and Sontag [1991], El-Farra and Christofides [2003] for a review, see Bequette [1991], Christofides and El-Farra [2005]) that provide an explicit characterization of the stability region in the presence of constraints as well as model predictive control designs (see, for example, Mayne and Michalska [1990], Muske and Rawlings [1993] and the survey paper, Mayne et al. [2000]) 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 (Mhaskar et al. [2005, 2006a]) that allow explicit characterization of the stability region in the presence of constraints, without assuming initial feasibility of the optimization problem. Several research efforts have also focused on the problem of control of switched systems; see Mhaskar et al. [2005] for a recent result on a control design that achieves stabilization while satisfying a prescribed switching schedule.

The control tools described above have been utilized within reconfiguration-based fault-tolerant control structures focusing on closed–loop stability and performance, while accounting for process nonlinearity and constraints (see, e.g., Mhaskar et al. [2006b], Mhaskar [2006], Mhaskar et al. [2008]). 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 Mhaskar [2006], Mhaskar et al. [2006b, 2008] 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 temporarily shutting down the process which can have substantially negative economic ramifications.

Motivated by the above considerations, this thesis considers the problem of control of nonlinear process systems subject to input constraints and destabilizing faults in the control actuators. Specifically, faults are considered that cannot be handled via robust control approaches or activation of redundant control configurations, and

necessitate fault-rectification. In Chapter 2, a safe-parking framework is developed to address the problem of determining how to run the process during fault-rectification to enable smooth resumption of nominal operation. First Lyapunov-based model predictive controllers, that allow for an explicit characterization of the stability region subject to constraints on the manipulated input, are designed. The stability region characterization is utilized in selecting 'safe-park' points from the safe-park candidates (equilibrium points subject to failed actuators). Specifically, a candidate parking point is termed a safe-park point if 1) the process state at the time of failure resides in the stability region of the safe-park candidate (subject to depleted control action), and 2) the safe-park candidate resides within the stability region of the nominal control configuration. This safe-park point is chosen as a temporary operating point where process is to be operated during fault rectification. This ensures that process can be safely operated during fault rectification and the nominal operation can be resumed upon fault recovery. When multiple candidate safe-park points are available, performance considerations, such as ease of transition from and to the safe-park point and cost of running the process at the safe-park point, are quantified and utilized in choosing the optimal safe-park point. The proposed framework is illustrated using a chemical reactor example and robustness with respect to parametric uncertainty and disturbances is demonstrated on a styrene polymerization process.

The safe-parking framework proposed in Chapter 2 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-recovery. Motivated by the

above considerations, Chapter 3 considers the problem of handling faults in control of nonlinear process systems subject to input constraints, uncertainty and unavailability of measurements. We first 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 recovery. 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.

The safe-parking framework proposed in Chapter 2 and Chapter 3 considers faults in isolated units, however, the opportunities and challenges that arise in a plant-wide setting due to the connected nature of chemical processes via material, energy or communication lines simply do not exist in an isolated unit. The results in Chapter 2 and Chapter 3 therefore cannot be applied to a plant-wide setting. In fact, a simple application of the results in Chapter 2 and Chapter 3 to a multi-unit setting can result in missed opportunities as well as inadequate safe-parking. In particular, when safe-parking a unit in a plant, the fact that the outlets from the faulty unit goes to another unit (where functioning manipulated inputs exist) can help in localizing

the effect of the fault to the faulty unit, and preserving nominal operation in the downstream plant. On the other hand, if the fact that a unit (when multiple units are being safe-parked) receives altered (or non-nominal) outlet streams from an upstream safe-parked unit is not accounted for, it can result in the inability to adequately safe-park the unit in question. In particular, a change in operating condition of one unit naturally acts as a disturbance to the downstream units and hence large changes in operating conditions of one unit, while possibly enabling safe-parking of the unit in question, can jeopardize the operation of the downstream units, and therefore of the whole plant. This necessitates that the safe-park point for a unit in multi-unit processes be chosen with adequate consideration of its effect on downstream units.

Motivated by the above considerations, Chapter 4 addresses the problem of handling faults in the context of multi-unit processes. We consider a multi-unit nonlinear process system subject to input constraints and actuator faults in one unit that preclude the possibility of operating the unit at its nominal equilibrium point. We first consider the case where there exists a safe-park point for the faulty unit such that its effect can be completely rejected (via changing the nominal values of the manipulated variables) in the downstream unit. Steady-state as well as dynamic considerations (including the presence of input constraints) are used in determining the necessary conditions for safe-parking the multi-unit system. We next consider the problem where no viable safe-park point for the faulty unit exists such that its effect can be completely rejected in the subsequent unit. A methodology is developed that allows simultaneous safe-parking of the consecutive units. Finally, we incorporate performance considerations in the safe-parking framework for the multi-unit processes. Efficacy of the safe-parking framework for plant-wide setting is demonstrated using

simulations study on a multi-unit chemical reactor system.

Next, we demonstrate efficacy of proposed Lyapunov based Model Predictive Controller and Safe-Parking framework on practical scale polymerization reactor model to control the polymerization reactor at an unstable equilibrium point and to handle faults that dont allow continuation of the nominal operation in the reactor. Polymerization processes are an important class of chemical processes. The plastic consumption of the world was estimated to be around 200 million tons in 2000 (Rosato et al. [2001]) and continues to grow at a substantial rate. Continuous polymerization reactors are widely used to produce synthetic polymer products such as styrene. The increasing demand for high quality polymers has given impetus to controller designs that provide good control of the polymer product properties and minimize off-spec product during the start-up and the grade transitions. As with most chemical processes, polymerization reactors are characterized by the presence of process nonlinearity, uncertainty and constraints. Over and above the inherent complexity of the process, operation has to deal with eventualities such as equipment and control algorithm faults, which, if not addressed in a timely manner, can lead to substantial economic losses and safety hazards motivating significant research on fault-tolerant control.

In Chapter 5, we address the problem of effective control of the styrene polymerization reactor (where living Nitroxide-Mediated Radical Polymerization of styrene takes place) at an unstable equilibrium point and also the problem of how to operate the reactor during fault-rectification for the faults that do not allow continuation of nominal operation in the reactor. First we design a Lyapunov based predictive controller for the styrene polymerization reactor in a way that allows for an explicit

characterization of the set of initial conditions from where the reactor can be stabilized. Then, we consider the problem of handling faults in the manipulated inputs. We design and implement the safe-parking framework to choose a safe-park point where the reactor can be operated during fault rectification. Upon fault recovery, the process states are driven back to the nominal operation. This ensures safe-operation and minimizes deviation from specs during fault rectification and smooth resumption of nominal operation upon fault recovery. Finally, in Chapter 6 conclusions and recommendations for future work is presented.

Bibliography

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

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.

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.

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

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

N. Huynh and N. Kazantzis. Parametric optimization of digitally controlled nonlinear reactor dynamics using zubov-like functional equations. *J. Math. Chem.*, 38:499–519, 2005.

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

C. Kravaris and S. Palanki. Robust nonlinear state feedback under structured uncertainty. *AIChE J.*, 34:1119–1127, 1988.

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

D. Q. Mayne and H. Michalska. Receding horizon control of nonlinear systems. *IEEE Trans. Automat. Contr.*, 35:814–824, 1990.

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.

P. Mhaskar. Robust model predictive control design for fault-tolerant control of process systems. *Ind. & Eng. Chem. Res.*, 45:8565–8574, 2006.

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.

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.*, 55:650–659, 2006a.

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, 2006b.

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.

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

Dominick V. Rosato, Nick R. Schott, and Marlene G. Rosator. *Plastics Engineering, Manufacturing & Data Handbook: Plastics Engineering, Manufacturing & Data Handbook.* Springer, 2001.

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

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.

Blank Page

Chapter 2

Safe-Parking of Nonlinear Process Systems [†]

2.1 Introduction

A Fault Tolerant Control System (FTSC) aims to maintain some "acceptable" level of performance of the system if possible or degrade gracefully on occurrence of fault. Here graceful degradation means going to a suboptimal operating point or to shutdown safely. The existing Fault Tolerant Control methodologies can be categorized within the robust/reliable, and reconfiguration-based fault-tolerant control approaches. Robust/reliable control approaches (e.g., see Wang et al. [1999]) essentially rely on the robustness of the active control configuration to handle faults as disturbances. Several faults, however, cause significant erosion of the control effort in the active control configuration, and closed-loop stability cannot be preserved by

[†]The results in this chapter are published in "R. Gandhi and P. Mhaskar, Safe-parking of nonlinear process systems, *Comp. and Chem. Eng.*, 32:2113-2122, 2008".

simply re-tuning the controller in the active control configuration. If redundant control configurations are available, control–loop reconfiguration (activating an appropriately chosen fall-back configuration) can be implemented to preserve closed–loop stability at the nominal equilibrium point. However, all existing methods for handling faults, whether robust or reconfiguration based fault tolerant control approach, assume availability of sufficient residual control effort or redundant control configurations to preserve operation at the nominal equilibrium point. The scenario where due to fault, the nominal operating point ceases to be an equilibrium point has not been explicitly addressed. In the absence of a framework for handling such faults, ad-hoc approaches could result in temporarily shutting down the process which can have substantially negative economic ramifications.

Motivated by the above considerations, this chapter considers the problem of control of nonlinear process systems subject to input constraints and destabilizing faults in the control actuators. Specifically, faults are considered that cannot be handled via robust control approaches or activation of redundant control configurations, and necessitate fault-rectification. A safe-parking framework is developed to address the problem of determining how to run the process during fault-rectification to enable smooth resumption of nominal operation.

The rest of the chapter is organized as follows: we first present, in Section 2.2.1, the class of processes considered, followed by a styrene polymerization process in Section 2.2.7 and review a Lyapunov-based predictive controller in Section 2.2.6. The safe-parking problem is formulated in Section 2.3.1, and safe-parking designs that address stability and performance objectives are presented in Sections 2.3.2 and 2.3.3, respectively. A chemical reactor example is used to illustrate the details of the safe-parking

framework in Section 2.3.4 while application to the styrene polymerization process, subject to parametric uncertainty and disturbances, is demonstrated in Section 2.4. Finally, in Section 2.5 we summarize our results.

2.2 Preliminaries

In this section, we first describe the class of processes considered and then review theory of nonlinear control systems, stability analysis of nonlinear controllers, Model Predictive Controller and a Lyapunov-based model predictive control design. We also present a polystyrene process example to motivate the proposed framework.

2.2.1 Process description

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

$$\dot{x}(t) = f(x(t)) + G(x(t))u_\sigma(t), \quad u_\sigma(\cdot) \in \mathbf{U} \tag{2.1}$$

where $x \in \mathbb{R}^n$ denotes the vector of state variables, $u_\sigma(t) \in \mathbb{R}^m$ denotes the vector of constrained manipulated inputs, taking values in a nonempty convex subset $\mathbf{U}$ of $\mathbb{R}^m$, where $\mathbf{U} = \{u \in \mathbb{R}^m : u_{min} \leq u \leq u_{max}\}$, where $u_{min}, u_{max} \in \mathbb{R}^m$ denote the constraints on the manipulated inputs, $f(0) = 0$ and $\sigma \in \{1, 2\}$ is a discrete variable that indexes the fault-free and faulty operation ($\sigma = 1$ denotes fault-free operation and $\sigma = 2$ denotes faulty operation). The vector functions $f(x)$ and the matrix $G(x) = [g^1(x) \cdots g^m(x)]$ where $g^k(x) \in \mathbb{R}^n$, $k = 1 \cdots m$ are assumed to be sufficiently smooth on their domains of definition. The notation $\|\cdot\|_Q$ refers to the

weighted norm, defined by $\|x\|_Q^2 = x'Qx$ for all $x \in \mathbb{R}^n$, where Q is a positive definite symmetric matrix and x' denotes the transpose of x. Throughout the chapter, we assume that for any $u \in \mathbf{U}$ the solution of the system of Eq.2.1 exists and is continuous for all t, and in this chapter we focus on the state feedback problem where $x(t)$ is assumed to be available for all t.

2.2.2 Lyapunov function

The Lyapunov functions are scalar functions which can be used to prove the stability of a certain fixed point in a dynamical system. The basic philosophy of the Lyapunov function is to define a scalar function of the system states that captures the total energy of a mechanical (or electrical) system which is continuously dissipated. If there exists such a function then the system, whether linear or nonlinear, must eventually settle down to an equilibrium point and thus system is stable. A Lyapunov function gives sufficient condition for stability, asymptotic stability, and so on. In general, stability analysis using the Lyapunov function is applicable to autonomous systems.

Control Lyapunov Function (CLF)

The Control Lyapunov Function (CLF) is a generalization of the concept of Lyapunov function, and can be applied to system with exogenous inputs (u) to test whether the system is feedback stabilizable, that is whether for any state x there exists a control action $u(x,t)$ such that the system can be brought to the zero by applying the control law $u(x,t)$. In other words, it says that for each point in state space (x), we can find a control (u) that will reduce the "energy" ($V(x)$), and as a result the energy will eventually go to zero, that is to bring the system to the origin.

As with the Lyapunov function, there is no general procedure to find a control Lyapunov function for any given system but, fortunately, there is a sizeable class of systems for which the systematic construction of a CLF is possible (feedback linearizable, strict feedback and feed-forward systems, etc., see Nevisti et al. [1999] for details). Alternately, a local quadratic Control Lyapunov Function, $V(x) = x^T Px$ (valid in the region around the equilibrium point) can be constructed by solving the following Riccati equation for P (Dorato et al. [2000]),

$$A^T P + PA - PBB^T P + Q = 0 \tag{2.2}$$

where $A = \frac{df(x)}{dx}|_{x=x_{eq}}$, $B = \frac{dG(x)}{dx}|_{x=x_{eq}}$ and P and Q are positive definite matrices. If P is a positive definite matrix then the control Lyapunov function $V(x) = x^T Px$ can be constructed and this ensures that system is feedback stabilizable in the neighborhood of the origin.

2.2.3 Stability region

The stability region (also referred as stability domain) for a nonlinear dynamical systems is defined as a set of state space points from where the dynamical system can be stabilized to the origin using the given control law and bounds on inputs. In this work, we use the Lyapunov function based approach to estimate the stability region.

Let $V : \mathbb{R}^n \rightarrow \mathbb{R}$ be a (control) Lyapunov function for the system defined in Eq.2.1. Further define a set

$$\Pi = \{x \in \mathbb{R}^n : \exists u \in U \text{ such that } \dot{V}(x,u) \leq 0\} \tag{2.3}$$

In other words, for all state space points in the set Π there exists an admissible control action such that the Lyapunov function can be made to decrease. Now let us define a set Ω which is the biggest sub level set of the Lyapunov function such that $\Omega \subseteq \Pi$.

$$\Omega = \{x \in \mathbb{R}^n : V(x) \leq c^{max}\} \tag{2.4}$$

Having defined Ω, now consider any trajectory starting from an arbitrary point $x_0 \in \Omega$. If the control law for the nonlinear system is designed to choose a control action such that $\dot{V}(x) < 0$ (which is a feasible control law for any point x inside Ω from the definition of Ω), then the trajectory remains inside Ω for all time and the closed loop system is asymptotically stable (because $\dot{V}(x(t)) < 0$ for $t > 0$ implies that $V(x(t+\Delta)) < V(x(t)) < V(x(0)) < c^{max}$). Thus, Ω can act as a stability region for any controller that forces continuous decrease in Lyapunov function i.e. the controller can stabilize the system from any point inside Ω to the origin. The size of the stability region depends on the constraints on the inputs and on the choice of the Lyapunov function.

Stability region characterization

In this subsection, we describe computational details for characterizing the stability region (Ω). The goal is to estimate the biggest sub level set of the Lyapunov function $V(x) = c^{max}$, $\forall x$ such that $V(x) < c^{max}$, we can find admissible input ($u \in U$) so that $\dot{V}(x,u) < 0$. $\dot{V}(x,u)$ can be given as,

$$\begin{aligned}\dot{V}(x,u) &= \frac{dV}{dx}\dot{x} = \frac{dV}{dx}\{f(x(t)) + G(x(t))u(t)\} \\ &= L_f V(x) + L_G V(x)u(t) = L_f V(x) + \sum_{i=1}^{m} L_{g^i} V(x)u^i(t) \end{aligned} \tag{2.5}$$

Where $L_f V(x) = \frac{dV}{dx} f(x(t))$ and $L_g V(x) = \frac{dV}{dx} g(x(t))$. The notation $L_f h$ denotes the standard Lie derivative of a scalar function $h(\cdot)$ with respect to the vector function $f(\cdot)$. For a given state space point x, it can be verified whether $\dot{V}(x,u) < 0$ or not by using following control law:

$$u^i = \left\{ \begin{array}{rcl} u^i_{max} & , & L_{g^i} V(x) < 0 \\ u^i_{min} & , & L_{g^i} V(x) > 0 \\ 0 & , & L_{g^i} V(x) = 0 \end{array} \right\} \tag{2.6}$$

The control law choses u^i such that value of $L_{g^i} V(x)u^i$ term is the most negative, thus giving most possible negative value of $\dot{V}(x,u)$ for the given x and the constraints on the inputs. In this work, a grid search technique is used to estimate the stability region. All the dimensions of the state space are discretized in uniform intervals to create a grid and then for all points on the grid, $\dot{V}(x,u)$ is evaluated using the control law of Eq.2.6. If $\dot{V}(x,u) < 0$, then the state space point is included in the set Π. For two dimensional system, the a typical set Π is shown in Fig.2.1 by the dotted region.

Once the set Π is characterized, biggest level set of the Lyapunov function is fitted inside the set Π. For two dimensional case, this can be achieved through visual inspection. The level sets of the Lyapunov functions are superimposed on the set Π

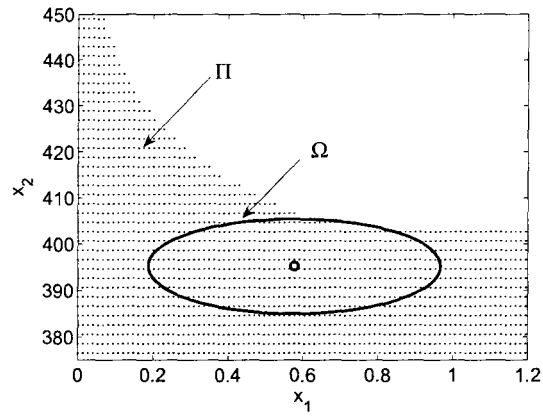


Figure 2.1: Illustration of stability region characterization using grid search technique. Dotted region represents the set Π and the ellipse (Ω) represents the biggest level set of the Lyapunov function that fits inside the set Π

to verify whether the level set is completely contained inside the set Π or not. In Fig.2.1, a biggest level set (Ω) that is contained in the set Π is shown. For systems with more than two dimension, the visual inspection is not straight forwards and more complex algorithms needs to be used. Aumi and Mhaskar [2009] uses multiple projections of n dimensional ellipsoid on two dimension planes in the conjunction with visual inspection to verify $\Omega \subset \Pi$.

2.2.4 Model Predictive Controller (MPC)

Model Predictive Controller (MPC) refers to a class of algorithms that computes a sequence of manipulated variable adjustments in order to optimize the future behavior of a plant (Qin and Badgwell [1998]). To achieve this, MPC can use various kind of models to predict behavior of outputs i.e. first principle model, empirical model, linear model, nonlinear model etc. and based on the type of model the MPC uses, there are various types of MPC formulations available in the literature.

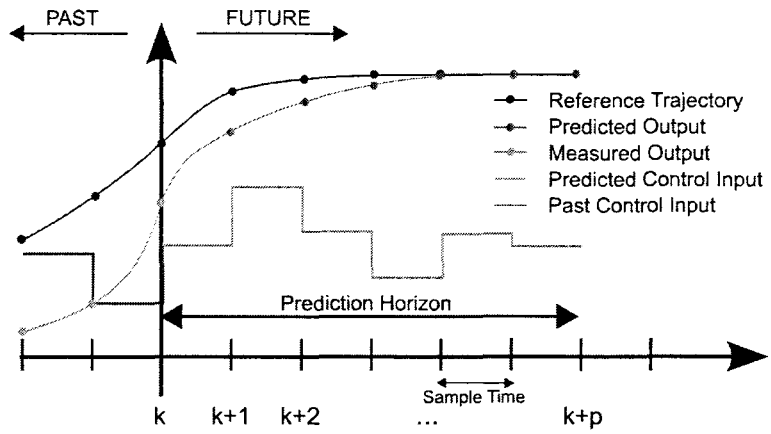


Figure 2.2: Basic idea of Model Predictive Controller (MPC) (Figure taken from Wikipedia article on "Model Predictive Controller")

The basic idea of Model Predictive Controller is shown in Fig.2.2. It can be seen that the manipulated variables have been adjusted in the past and so while making prediction of the controlled output, the effect of this past manipulation, and also the effect of disturbances, is considered. In Fig.2.2, predicted control input and prediction of controlled output is shown. The task of the control algorithm is to determine future adjustments to the manipulated variables that will make predicted controlled variable to follow the reference trajectory as close as possible (by solving the optimization problem of Eqs.2.7-2.10).

$$\min_{u_i,\, i=k:k+p-1} J_k(x, u(\cdot)) = \sum_{i=k}^{k+p} [\|x(i)\|_{Q_w} + \|u(i)\|_{R_w}] + V_f(x(k+p)) \tag{2.7}$$

$$\text{subject to: Process model} \tag{2.8}$$

$$x(i) \in X,\ \forall i = k : k+p \tag{2.9}$$

$$u(i) \in U,\ \forall i = k : k+p \tag{2.10}$$

Model predictive controller solves the optimization problem of Eqs.2.7-2.10 every instant and the first control move is implemented on the process system and this process is repeated indefinitely. Here $J_k(x, u(\cdot))$ is the MPC objective function, $V(x(k+p))$ is terminal penalty function, X is a set of allowable values of process states (x), U is the set of allowable values of inputs (u). The matrices Q_w and R_w are weightings and p is prediction horizon.

The major advantages of Model Predictive Controller over traditional multi-loop PID control system is that it can automatically compensate for process interactions, measurable load disturbances and difficult dynamics. It is also capable of handling constraints on controlled variables, state variables and manipulated variables.

The research in the field of MPC is relatively mature with abundant theoretical and practical results available for the stability and performance of MPC (Mayne et al. [2000]). The performance and stability of MPC depends on various tuning parameters including R, Q, prediction horizon (p), control horizon etc. Choice of optimal tuning parameters to ensure both performance and stability is not straight forward and no general guidelines are available, though many researchers have attempted to solve this problem (see Al-ghazzawi et al. [2001] and references therein). Longer prediction horizon generally improves the stability property of MPC but it also increases computational cost for solving MPC optimization problem. Alternately, stability and performance of controller can be decoupled by including explicit stability constraint in the MPC optimization problem. Including stability constraints in optimization problem of Eqs.2.7-2.10 puts stability before performance and this strategy is not popular in Linear MPC, but for nonlinear MPC (see Section 2.2.5), where longer prediction

horizon to ensure stability can make problem intractable in real time, the stability constraints are frequently used. There are various types of stability constraints proposed in the literature and are discussed briefly in the next section.

2.2.5 Nonlinear Model Predictive Controller (NMPC)

In this section, we briefly discuss stability properties of Nonlinear Model Predictive Controller that uses nonlinear process model of the form of Eq.2.1 to make the predictions.

The main challenge in nonlinear MPC is to guarantee closed loop stability and performance with prediction horizon (p) as short as possible due to computational reasons. Many researcher have proposed various NMPC formulations with different forms of terminal penalty ($V_f(x(k+p))$) and stability constraints (also called terminal constraints). Terminal constraints are usually in following form:

$$x(k+p) \in X_f \tag{2.11}$$

where $X_f \subset R^n$ is the set where process states are required to reside at end of prediction horizon. Some of the NMPC formulations are reviewed below (see Nicolao et al. [1999] for more details on stability of NMPC):

The Zero terminal constraint (Chen and Shaw [1982], Mayne and Michalska [1990])

The idea here is to let $V_f(x) = 0$ and $X_f = \{0\}$ i.e. $x(t+p) = 0$. For this controller the stability region coincides with the controllability region ($X^c(p)$) and $X^c(p)$ grows with p, but increasing prediction horizon (p) has computational drawback. Zero terminal

constraint MPC guarantees feasibility from any state inside $X^c(p)$.

Dual mode controller (Michalska and Mayne [1993])

This controller uses terminal constraint of $x(t+p) \in W_\alpha$ where W_α denotes the stability region (output admissible set) of LQ controller (in other words W_α is invariant set for LQ controller) where α is a scalar parameter such that $W_{\alpha''} \supset W_{\alpha'}$ if $\alpha'' < \alpha'$ and $\lim_{\alpha \to 0}\{0\}$. At time $t+p$ (when $x(t+p) \in W_\alpha$) the controller switches to linear state feedback. The stability region $X^{DM}(p, \alpha)$ grows with p and α.

The Contractive constraints (Yang and Polak [1993])

Here the terminal constraint is defined as a contractive constraint of the type,

$$X_f = \{x(t+p) | \|x(t+p)\| \leq \alpha \|x(t)\|\}, \alpha \in [0,1] \tag{2.12}$$

Here a further constraint is also introduced to be satisfied at each time within the optimization horizon,

$$\|x(t+i)\| \leq \beta \|x(t)\|, \ 1 \leq i \leq N, \ \beta \in (1, \infty) \tag{2.13}$$

Here α and β are design parameters.

Lyapunov terminal constraint

As name suggests, here the terminal constraint is defined in terms of Lyapunov function. It requires that control action be calculated such that the Lyapunov function

decreases continuously,

$$\dot{V}(x(t), u(t)) < 0, \quad t > 0 \tag{2.14}$$

There are many variants of the Lyapunov terminal constraints that differ from implementation point of view, but the basic idea remain same. In this work, we will use nonlinear model predictive controller that uses Lyapunov terminal constraint to guarantee stability of closed loop system.

2.2.6 Lyapunov-based model predictive control

In this section, we briefly review a recent result on the design of a Lyapunov-based predictive controller that uses the Lyapunov terminal constraints presented in previous section. In Section 2.2.3, we defined set Ω that can act as stability region for any controller that forces continuous decrease in the Lyapunov function. A similar idea is used here for designing a controller that possesses an explicitly characterized set of initial conditions from where it is guaranteed to be feasible, and hence stabilizing in the presence of input constraints.

Consider the system of Eq.2.1, for $\sigma(t) = 1$ (i.e., under no fault, where all the manipulated inputs can be changed via a feedback law), under the predictive controller

(Mhaskar et al. [2005b]) of the form:

$$u_1(\cdot) = argmin\{J(x,t,u(\cdot))|u(\cdot) \in S\} \tag{2.15}$$

$$s.t.\ \dot{x} = f(x) + G(x)u(t) \tag{2.16}$$

$$\dot{V}(x(\tau)) \leq -\epsilon^*\ \forall\ \tau \in [t, t+\Delta)\ if\ \ V(x(t)) > \delta' \tag{2.17}$$

$$V(x(\tau)) \leq \delta'\ \forall\ \tau \in [t, t+\Delta)\ \ if\ \ V(x(t)) \leq \delta' \tag{2.18}$$

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.2.16 is the nonlinear model describing the time evolution of the state x, V is a control Lyapunov function and δ', ϵ^* are parameters to be determined. A control $u(\cdot)$ in S is characterized by the sequence $\{u[j]\}$ where $u[j] := u(j\Delta)$ and satisfies $u(t+\tau) = u[j]$ for all $\tau \in [t+j\Delta, t+(j+1)\Delta)$. The performance index is given by

$$J(x,t,u(\cdot)) \ = \ \int_t^{t+T} \left[\|x^u(s;x,t)\|^2_{Q_w} + \|u(s)\|^2_{R_w}\right] ds \tag{2.19}$$

where Q_w is a positive semi-definite symmetric matrix and R_w is a strictly positive definite symmetric matrix. $x^u(s;x,t)$ denotes the solution of Eq.2.1, due to control u, with initial state x at time t. The minimizing control $u[1] \in S$ is then applied to the plant over the interval $[t, t+\Delta)$ and the procedure is repeated indefinitely.

For this Lyapunov based MPC, we characterize stability properties using a bounded controller of the form (e.g., see Lin and Sontag [1991], El-Farra and Christofides [2003]):

$$u(x) \ = \ -k(x)(L_G V)'(x) \tag{2.20}$$

$$k(x) = \frac{L_f V(x) + \sqrt{(L_f V(x))^2 + (u_{max}\|(L_G V)'(x)\|)^4}}{\|(L_G V)'(x)\|^2 \left[1 + \sqrt{1 + (u_{max}\|(L_G V)'(x)\|)^2}\right]} \tag{2.21}$$

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.2.20–2.21, one can show, that whenever the closed–loop state, x, evolves within the region described by the set:

$$\Pi = \{x \in \mathbb{R}^n : L_f V(x) \leq u^{norm}\|(L_G V)'(x)\|\} \tag{2.22}$$

where $u^{norm} > 0$ is such that $\|u\| \leq u^{norm}$ implies $u \in \mathbf{U}$, where $\|(\cdot)\|$ denotes the Euclidean norm of a vector, then the control law satisfies the input constraints, and the time-derivative of the Lyapunov function is negative-definite. Note that the set Π defined in Section 2.2.3 is controller independent, but the set Π defined in Eq. 2.22 is specific to bounded control law of Eqs. 2.20-2.21.

Similar to Section 2.2.3, an estimate of the stability region can be constructed using the biggest level set of the Lyapunov function $V(x)$,

$$\Omega = \{x \in \mathbb{R}^n : V(x) \leq c^{max}\} \tag{2.23}$$

where $c^{max} > 0$ is the largest number for which $\Omega \subseteq \Pi$. Closed–loop stability and feasibility properties of the closed–loop system under the Lyapunov–based predictive controller are inherited from the bounded controller under discrete implementation and are formalized in Theorem 2.1 below (for a proof, see Mhaskar et al. [2005b]).

Theorem 2.1. (Mhaskar et al. [2005b]) *Consider the constrained system of Eq.2.1 under the MPC law of Eqs.2.15–2.19. Then, given any* $d \geq 0$, $x_0 \in \Omega$, *where* Ω *was defined in Eq.2.23, there exist positive real numbers* δ', ϵ^*, Δ^*, *such that if* $\Delta \in (0, \Delta^*]$, *then the optimization problem of Eq.2.15-2.19 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 predictive controller formulation of Eqs. 2.15–2.19 requires that the value of the Lyapunov function decrease during the first step only. Practical stability of the closed–loop system is achieved since only the first move of the set of calculated moves is implemented and the problem is re-solved at the next time step. If the optimization problem is initially feasible and continues to be feasible, then every control move that is implemented enforces a decay in the value of the Lyapunov function, leading to stability. Furthermore, the constraint of Eq.2.17 is guaranteed to be satisfied since the control action computed by the bounded controller design provides a feasible initial guess to the optimization problem. Finally, since the state is initialized in Ω, which is a level set of V, the closed–loop system evolves so as to stay within Ω, thereby guaranteeing feasibility at future times. The key idea in the predictive control design is to identify stability constraints that can a) be shown to be feasible and b) upon being feasible can guarantee stability. Note that the model predictive controller of Eqs. 2.15–2.19 is only used to illustrate the safe-parking framework, and any other controller that provides an explicit characterization of the closed–loop stability region can be used within the proposed framework.

2.2.7 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 a model for a polystyrene polymerization process given in Hidalgo and Brosilow [1990] (also studied in, e.g., Prasad et al. [2002])

$$\begin{aligned}
\dot{C}_I &= \frac{(F_i C_{If} - F_t C_I)}{V_{pr}} - k_d C_I \\
\dot{C_M} &= \frac{(F_m C_{Mf} - F_t C_M)}{V_{pr}} - k_p C_M C_P \\
\dot{T} &= \frac{F_t(T_f - T)}{V_{pr}} + \frac{(-\Delta H)}{\rho c_p} k_p C_M C_P - \frac{hA}{\rho c_p V}(T - T_c) \\
\dot{T}_c &= \frac{F_c(T_{cf} - T_c)}{V_c} + \frac{hA}{\rho_c C_{pc} V_c}(T - T_c)
\end{aligned}$$

$$\begin{aligned}
C_P &= \left[\frac{2fk_dC_I}{k_t}\right]^{\frac{1}{2}} \\
k_d &= A_d e^{\frac{-E_d}{RT}} \\
k_p &= A_p e^{\frac{-E_p}{RT}} \\
k_t &= A_t e^{\frac{-E_t}{RT}}
\end{aligned} \tag{2.24}$$

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_c and T_{cf} refer to the coolant jacket and inlet temperatures, respectively. The 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 (Hidalgo and Brosilow [1990]), 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.

Table 2.2: 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	=	0.0480	kmol/m^3
$C_{Mf,n}$	=	9.975	kmol/m^3
C_M	=	2.3331	kmol/m^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}	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

The control objective is to stabilize the reactor at the equilibrium point (C_I = 0.067 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 = 0.131 L/s and F_m = 0.105 L/s. The manipulated inputs are constrained as $0 \leq F_m \leq 3.105$ L/s and $0 \leq F_c \leq 3.1$ 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. The key problem is to determine how to operate the process under failure condition so that upon fault-recovery, nominal operation can be resumed efficiently. We will demonstrate the application as well as investigate the robustness of the proposed safe-parking framework via the styrene polymerization process in Section 2.4, while illustrating the details of the proposed framework using an illustrative chemical reactor in Section 2.3.4.

2.3 Safe-parking of nonlinear process systems

We first formalize the problem in Section 2.3.1, and present a safe-parking algorithm focusing on closed–loop stability in Section 2.3.2. We then incorporate performance considerations in the safe-parking framework in Section 2.3.3.

2.3.1 Problem definition

We consider faults where one of the control actuators fails and reverts to the fail-safe value. Examples of fail-safe positions include fully open for a valve controlling a coolant flow rate, fully closed for a valve controlling a steam flow etc. (generalization to the case where multiple actuators fail and get 'stuck' at non-nominal values is discussed in Remark 2.4). Specifically, we characterize the fault occurring w.l.o.g., in the first control actuator at a time T^{fault}, subsequently rectified at a time $T^{recovery}$ (i.e., for $t \leq T^{fault}$ and $t > T^{recovery}$, $\sigma(t) = 1$ and $\sigma(t) = 2$ for $T^{fault} < t \leq T^{recovery}$), as $u_2^1(t) = u_{failed}^1$, with $u_{min}^1 \leq u_{failed}^1 \leq u_{max}^1$, where u^i denotes the ith component of a vector u, for all $T^{fault} < t \leq T^{recovery}$, leaving only u_2^i, $i = 2 \ldots m$ 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 equilibrium points that the system can be stabilized at, subject to the failed actuator, and with the other manipulated inputs within the allowable ranges. Note that if $u_{failed}^1 \neq 0$, then it may happen that $0 \notin X_c$, i.e., if the failed actuator is frozen at a non-nominal value, then it is possible that the process simply cannot be stabilized at the nominal equilibrium point using the functioning control actuators. 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 drive the process state to a point from where it may not be possible to resume nominal operation upon fault-recovery,

or even if possible, may not be 'optimal'. We define the safe-parking problem as the one of identifying safe-park points $x_s \in X_c$ that allow efficient resumption of nominal operation upon fault-recovery.

2.3.2 Safe-parking to resume nominal operation

In this section, we present a safe-parking framework and a controller that executes safe-parking as well as resumption of nominal operation. To account for the presence of constraints on the manipulated inputs, the key requirements for a safe-park point include that the process state at the time of the failure resides in the stability region for the safe-park point (so the process can be driven to the candidate safe-park point), and that the safe-park point should reside in the stability region under nominal operation (so the process can be returned to nominal operation). These requirements are formalized in Theorem 2.2 below. To this end, consider the system of Eq.2.1 for which the first control actuator fails at a time T^{fault} and is reactivated at time $T^{recovery}$, and for which the stability region under nominal operation, denoted by Ω_n, has been characterized using the predictive controller formulation of Eqs.2.15–2.19. Similarly, for a candidate safe-park point x_c, we denote Ω_c as the stability region (computed a priori) under the predictive controller of Eqs.2.15–2.19, and u_{2,x_c} as the control law designed to stabilize at the candidate safe-park with $u_{1,n}$ being the nominal control law.

Theorem 2.2. *Consider the constrained system of Eq.2.1 under the MPC law of Eqs.2.15–2.19. If $x(T^{fault}) \in \Omega_c$ and $\Omega_c \subset \Omega_n$, then the switching rule*

$$u(t) = \left\{ \begin{array}{lll} u_{1,n} & , & 0 \leq t < T^{fault} \\ u_{2,x_c} & , & T^{fault} \leq t < T^{recovery} \\ u_{1,n} & , & T^{recovery} \leq t \end{array} \right\} \tag{2.25}$$

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

Proof of Theorem 2.2: We consider the two possible cases; first if no fault occurs ($T^{fault} = T^{recovery} = \infty$), and second if a fault occurs at a time $T^{fault} < \infty$ and is recovered at a time $T^{fault} \leq T^{recovery} < \infty$.

Case 1: The absence of a fault implies $u(t) = u_{1,n} \; \forall \; t \geq 0$. Since $x(0) \in \Omega_n$, and the nominal control configuration is implemented for all times, we have from Theorem 2.1 that $x(t) \in \Omega_n \; \forall \; t \geq 0$ and $\limsup_{t \to \infty} \|x(t)\| \leq d$.

Case 2: At time T^{fault}, the control law designed to stabilize the process at x_c is activated and implemented till $T^{recovery}$. Since $x(T^{fault}) \in \Omega_c \subset \Omega_n$, we have that $x(t) \in \Omega_n \; \forall \; T^{fault} \leq t \leq T^{recovery}$. At a time $T^{recovery}$, we therefore also have that $x(T^{recovery}) \in \Omega_n$. Subsequently, as with case 1, the nominal control configuration is implemented for all time thereafter, we have that $x(t) \in \Omega_n \; \forall \; t \geq T^{recovery}$. In conclusion, we have that $x(t) \in \Omega_n \; \forall \; t \geq 0$ and $\limsup_{t \to \infty} \|x(t)\| \leq d$. This completes the proof of Theorem 2.2.

Remark 2.2. The statement of Theorem 2.2 requires that for a safe-park point, the stability (and invariant) region be such that the process state at the time of the failure resides in the stability region for the safe-park point so the process can be driven to the point of safe-park with the depleted control action available. Note that this characterization can be done off-line. Specifically, for a fail-safe position of an

actuator, the entire set of candidate safe-park points X_c can be computed off-line, and also, for any given point in this set, the stability region subject to depleted control action can also be computed off-line (as is done for the nominal equilibrium point). The statement of the theorem also requires that the stability (and invariant) region for a safe-park point be completely contained in the stability region under nominal operation, so the state trajectory always stays within the stability region under nominal operation. This requirement can be readily relaxed to only require that the state at the time of the failure reside in the stability region of the safe-park point. This will allow for the state trajectory to leave the stability region under nominal operation, and it may happen that at the time of fault-recovery, the closed–loop state trajectory does not reside in the stability region under nominal operation. However, to preserve closed–loop stability upon fault-recovery, the control law utilizing depleted control action may be continued up until the time that the state trajectory enters the stability region under nominal operation (this is guaranteed to happen because $x_c \in \Omega_n$), after which the control law utilizing all the manipulated inputs can be implemented to achieve closed–loop stability.

Remark 2.3. The key motivation, from a resumption of nominal operation stand point, for safe-parking is as follows: in the absence of a safe-park framework, if the control law still tries to utilize the available control action to preserve operation at the nominal operating point, the active actuators may saturate and drive the process state to a point starting from where resumption of nominal operation, even after fault-recovery, may not be achievable. Note that if continued operation at 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 Mhaskar [2006]) could be utilized. However, Theorem 2.2 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 2.4. Note that the assumption that the failed actuator reverts to the fail-safe position allows enumerating the possible fault situations for any given set of manipulated inputs a-priori to determine the safe-park candidates and then pick the appropriate safe-park point online (the condition $x_s \in \Omega_n$ can be verified off-line, however $x(T^{fault}) \in \Omega_{x_s}$ can only be verified online, upon fault-occurrence; for further discussion on this point, see Remark 2.5). The assumption reflects the 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). In the unlikely event that the actuators experience a mechanical failure and are not able to revert to a fail-safe position, one can work with simplified (albeit without guarantees) estimates of the stability regions that can be generated much faster (and therefore computed online, upon fault-occurrence), to implement the proposed safe-parking mechanism. Specifically, instead of stability regions estimated by constructing invariant sets Ω within the set of initial conditions Π for which the Lyapunov-function can be made to decay, one can use the set Π (which is much easier to compute) to implement the proposed safe-park mechanism (see Section 2.4 for a demonstration). Note also that while the statement of Theorem 2.2 considers faults in one of the actuators, generalizations to multiple faults (simultaneous or otherwise)

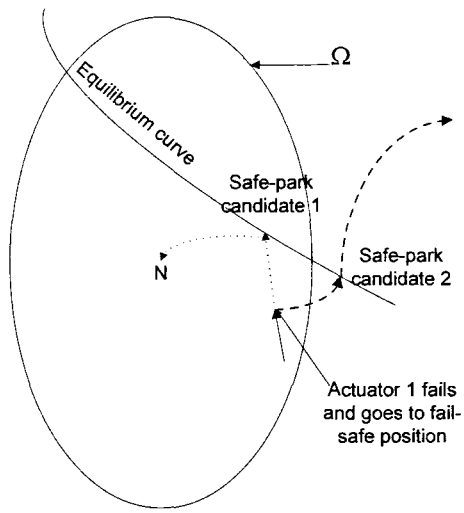


Figure 2.3: A schematic illustrating the safe-parking framework for a process with two actuators. Ω denotes the stability region under nominal operation. Solid line (—) shows the manifold of equilibrium points corresponding to the fail-safe value of the first actuator, and admissible values of the second actuator. Arbitrarily choosing a safe-park candidate (e.g., safe-parking candidate 2) does not guarantee resumption of nominal operation upon fault-recovery (see dashed lines "- -"), while choosing safe-park candidate 1 guarantees resumption of nominal operation upon fault-recovery (see doted lines "$\cdots$").

are possible, albeit involving the expected increase in off-line computational cost (due to the necessity of determining the safe-park points for all combinations of the faults in the control actuators).

Remark 2.5. The presence of constraints on the manipulated inputs limits the set of initial conditions from where the process can be driven to a desired equilibrium point. Control designs that allow an explicit characterization of their stability regions, and their use in deciding the safe-park point is therefore critical in determining the viability of a candidate safe-park point. Note also that while the schematic in Fig.2.3 shows two dimensional representations of the stability region to enable visual

verification of the presence of a candidate safe-park point in the stability region, the visual representation is *not* necessary. Specifically, the presence of a point in the stability region can be verified by evaluating the Lyapunov function value. Note that while the proposed safe-parking framework assumes *apriori* knowledge of the fail-safe positions of the actuators, it does not require a priori knowledge of the fault and recovery times, and only provides appropriate switching logic that is executed when and if a fault takes place and is subsequently rectified.

Remark 2.6. While the results in the present chapter are presented using the Lyapunov-based MPC of Eqs.2.15–2.19, the use of this controller is not critical to the implementation of the proposed safe-parking design. Any other control law that provides an explicit characterization of the stability region subject to constraints can be used instead to implement the proposed safe-parking framework. With respect to the design of the Lyapunov-based predictive controller of Eqs.2.15–2.19, we also note that while the use of a control Lyapunov function provides a better estimate of the stability region, even a quadratic Lyapunov function (chosen such that it is locally a control Lyapunov function) can be used to generate (possibly conservative) estimates of the stability region. For further discussion on this issue, see Mhaskar et al. [2005a].

Remark 2.7. Implicit in the implementation of the proposed safe-parking mechanism is the assumption of the presence of fault-detection and isolation filters. Existing results on the design of fault-detection filters include those that use past plant-data and those that use fundamental process models. Statistical and pattern recognition techniques for data analysis and interpretation (e.g., Rollins and Davis [1992], Davis et al. [1999], Yoon and MacGregor [2001], Zhang et al. [2004]) use past plant-data to construct indicators that identify deviations from normal operation to detect faults.

The analytical approach to fault detection relies on the use of fundamental models for the construction of residuals, that capture some measure of the difference between normal and 'faulty' dynamics, to achieve fault detection, isolation and estimation. The problem of using fundamental process models for the purpose of detecting faults has been studied extensively in the context of linear systems (Massoumnia et al. [1989], Frank [1990], Raich and Cinar [1995], Frank and Ding [1997], Mehranbod et al. [2005]); and more recently, results in the context of nonlinear systems have been derived (Saberi et al. [2000], DePersis and Isidori [2001], Mhaskar et al. [2008]). The proposed safe-parking framework determines the necessary course of action after a fault has been detected and isolated and can be readily integrated with any of the existing fault-detection and isolation structures.

2.3.3 Incorporating performance considerations in safe-parking

In the previous section, the requirements for an equilibrium point to be denoted a safe-park point was provided. A large set of equilibrium points may qualify as safe-park points and satisfy the requirements in Theorem 2.2. In this section, we introduce performance considerations in the eventual choice of the 'optimal' safe-park point. To this end, consider again the system of Eq.2.1 for which the first control actuator fails at a time T^{fault} and is reactivated at time $T^{recovery}$, and for which the set of safe-park points, $x_s \in X_s$, have been characterized. For a given safe-park point (one that satisfies the requirements of Theorem 2.2), define the followings costs:

$$J_{tr} = \int_{T^{fault}}^{T^{fault}+T_s} \left[\|x^u(s;x,t)\|_{Q_{tr}^2} + \|u(s)\|_{R_{tr}^2} \right] ds \tag{2.26}$$

where Q_{tr} and R_{tr} are positive definite matrices, the subscript tr signifying that this

value captures the 'cost' associated with transitioning to the safe-park point, with T_s being the time required to go to a sufficiently close neighborhood of the safe-park point. This cost can be estimated on-line, upon fault-occurrence, by running fast simulations of the closed–loop system under the auxiliary controller of Eq.2.20 (for further discussion on this issue, see Remark 2.8). Similarly, define

$$J_s = f_s(x_s, u_s) \tag{2.27}$$

where $f_s(x_s, u_s)$ is an appropriately defined cost function and the subscript s denotes that this value captures the 'cost' associated with operating at the safe-park point. Unlike the cost in Eq.2.26, this cost does not involve an integration over time, and can be determined off-line. The framework allows for inclusion of (possibly nonlinear) costs associated with further unit operations that may have to be performed to recover useful products from the process operating at the safe-park point (for further discussion on this issue, see Remark 2.9). Finally, define

$$J_r = \int_{T_{recovery}}^{T_{recovery}+T_r} \left[\|x^u(s;x,t)\|_{Q_r^2} + \|u(s)\|_{R_r^2}\right] ds \tag{2.28}$$

where Q_r and R_r are positive definite matrices, with the subscript r signifying that this value captures the 'cost' associated with resuming nominal operation, with T_r being the time required to return to a sufficiently close neighborhood of the nominal operating point, and the integration performed with the safe-park point as the initial condition. Again, this cost can be estimated off-line by running simulations of the closed–loop system under the auxiliary controller of Eq.2.20. Consider now the safe-park points $x_{s,i} \in X_s, i = 1, \ldots, N_s$ where N_s is the number of safe-park points to be

evaluated for optimality and let $J_{x_{s,i}} = J_{tr,i} + J_{s,i} + J_{r,i}$, $i = 1, \ldots, N_s$.

Theorem 2.3. *Consider the constrained system of Eq.2.1 under the MPC law of Eqs.2.15–2.19. If* $x(T^{fault}) \in \Omega_{s,o}$ *and* $\Omega_{s,o} \subset \Omega_n$, *then the switching rule*

$$u(t) = \left\{ \begin{array}{lll} u_{1,n} & , & 0 \leq t < T^{fault} \\ u_{2,x_{s,o}} & , & T^{fault} \leq t < T^{recovery} \\ u_{1,n} & , & T^{recovery} \leq t \end{array} \right\} \tag{2.29}$$

guarantees that $x(t) \in \Omega_n$, $\forall\ t \geq 0$ *and* $\limsup_{t \to \infty} \|x(t)\| \leq d$. *Here* $o \in \{1, \ldots N_s\} = arg \min_{i=1,N_s} J_{x_{s,i}}$ *and* $\Omega_{s,o}$ *is stability region of the optimal safe-park point* $x_{s,o}$

Proof of Theorem 2.3: Any $x_{s,o}$ chosen according to Theorem 2.3 satisfies the requirements of Theorem 2.2. The stability results follow from the proof of Theorem 2.2.

Remark 2.8. Note that the cost of transitioning to the safe-park point J_{tr} can be estimated using the auxiliary controller of Eq.2.20 since the auxiliary controller achieves decay of the same Lyapunov function as that used in the predictive controller design. This cost has to be estimated on-line, because it depends on the process state at which the failure occurs (in the special case that faults occur after the process has been stabilized at the nominal operating points, this cost can also be computed off-line; see Section 2.4 for a demonstration). In contrast, the cost incurred in resuming nominal operation from the safe-park point can be computed off-line. Such a computation can be done by running simulations under the predictive controller to get a more accurate estimate of the 'cost'. Additional terms in J_{tr} and J_s can be readily

included to cater to the specific process under consideration. Furthermore, the contribution of the cost J_s to the total cost can be appropriately scaled utilizing reasonable estimates of fault-rectification times. Specifically, if the malfunctioned actuator is known to require significant time to be rectified, then this cost can be 'weighed' more to recognize the fact that the process will deliver substantial amount of product corresponding to the safe-park point under consideration. If, on the other hand, it is known that the fault can be rectified soon, then the cost involving the resumption to nominal operation J_r, or alternatively, the time required to resume nominal operation can be given increased weight.

Remark 2.9. For the 'product' being generated during safe-parking, further unit operations may be required, ranging from simple separations to further processing, all of which may have associated costs. Possible loss of revenue during safe-park can be incorporated in the estimate J_s. If the process is connected to further units downstream, then increased utility costs associated with downstream processing can also be accounted for in this cost. Finally, we note that the costs outlined here are only some of the representative costs, and the framework allows for incorporating costs/revenues that may be specific to the process under consideration.

Remark 2.10. Note that while the set of safe-parking points (satisfying the requirements of Theorem 2.2) could be a continuous manifold of equilibrium points, safe-parking points to be evaluated for optimality can be picked by discretizing the manifold. The minimization in determining the optimal safe-park point can then be carried out by a simple procedure of comparison of the cost estimates associated with the finite number of safe-parking candidates. Choosing a finer discretization in evaluating the safe-parking candidates could possibly yield improved closed–loop costs,

however, the approximations involved in the cost estimation (the cost of going to and returning from the safe-parking points are only approximately estimated using the auxiliary controller of Eq.2.20) could offset the benefits out of the finer discretization. Therefore, a balance has to be struck in picking the number of safe-parking points that will be evaluated for optimality that trades off the increased computational complexity, the approximations in cost estimation, and the improved performance derived out of the finer discretization.

2.3.4 Illustrative simulation example

We illustrate in this section the proposed safe-park framework 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:

$$\begin{aligned} \dot{C_A} &= \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{RT_R}} C_A \\ \dot{T_R} &= \frac{F}{V}(T_{A0} - T_R) + \frac{(-\Delta H)}{\rho c_p} k_0 e^{\frac{-E}{RT_R}} C_A + \frac{Q}{\rho c_p V} \end{aligned} \tag{2.30}$$

where C_A denotes the concentration of the species A, T_R denotes the temperature of the reactor, Q is the heat added to/removed from the reactor, V is the volume of the reactor, k_0, E, ΔH are the pre-exponential constant, the activation energy, and the enthalpy of the reaction and c_p and ρ are the heat capacity and fluid density in the reactor. The values of all process parameters can be found in Table 2.3. The control objective is to stabilize the reactor at the unstable equilibrium point $(C_A^s,\ T_R^s) = (0.447\ \text{Kmol/m}^3, 393\ \text{K})$. Manipulated variables are the rate of heat

input/removal, Q, and change in inlet concentration of species A, $\Delta C_{A0} = C_{A0} - C_{A0_s}$, with constraints: $|Q| \leq 32$ KJ/s and $0 \leq C_{A0} \leq 2$ Kmol/m^3. The heat input/removal Q consists of heating stream Q_1 and cooling stream Q_2 with the constraints on each as, 0 KJ/s $\leq Q_1 \leq 32$ KJ/s and -32 KJ/s $\leq Q_2 \leq 0$ KJ/s. The nominal operating point (N) corresponds to steady state values of the inputs $C_{A0} = 0.73$ Kmol/m^3 and $Q = 10$ KJ/s.

Table 2.3: Chemical reactor parameters and steady–state values.

V	=	0.1	m^3
R	=	8.314	KJ/(Kmol $\cdot$ K)
C_{A0_s}	=	0.73	Kmol/m^3
T_{A0_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	=	1000.0	Kg/m^3
F	=	100×10^{-3}	m^3/min
T_{Rs}	=	393	K
C_{As}	=	0.447	Kmol/m^3

For stabilizing the process at the nominal equilibrium point, the Lyapunov based MPC of Section 2.2.6 is designed using a quadratic control Lyapunov function of the form $V = x^T P x$. The matix $P = \begin{bmatrix} 4.32 & 0 \\ 0 & 0.004 \end{bmatrix}$ is generated by solving Riccati equation of Eq. 2.2 with $Q = \begin{bmatrix} 1 & 1 \times 10^{-2} \\ 1 \times 10^{-2} & 1 \times 10^{-8} \end{bmatrix}$ and making off-diagonal entries zero. The stability region is estimated using grid search technique as described in Section 2.2.3 with grid interval of 0.6 °C and 0.004 Kmol/m^3. The stability region

is denoted by Ω in Fig.2.4. 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 $0 \leq C_{A0} \leq 2$ Kmol/m^3 exists such that the nominal equilibrium point continues to be an equilibrium point of the process subject to the fault. For $Q_2 = -14.7$ KJ/s, $C_{A0} = 1.33$ Kmol/m^3 and $Q_2 = -4$ KJ/s, $C_{A0} = 1.27$ Kmol/m^3, the corresponding equilibrium points are $S_1 = (1.05$ Kmol/m$^3, 396$ K) and $S_2 = (0.93$ Kmol/m$^3, 393$ K), which we denote as safe-park candidates. For each of these safe-park candidates, we also design Lyapunov based MPC of Section 2.2.6 using $P = \begin{bmatrix} 12.56 & 0 \\ 0 & 0.049 \end{bmatrix}$ for S_1 and $P = \begin{bmatrix} 12.32 & 0 \\ 0 & 0.026 \end{bmatrix}$ for S_2. The matrices in the objective function (Eq. 2.19), are chosen as $Q_w = \begin{bmatrix} 72.72 & 0 \\ 0 & 1 \end{bmatrix}$ and $R_w = \begin{bmatrix} 640 & 0 \\ 0 & 0.67 \end{bmatrix}$. Prediction and control horizons of 0.10 min and 0.02 min, respectively, are used in implementing the predictive controller. It should be noted that as the stability of closed loop process system is guaranteed by use of the stability constraint in the controller formulations, short prediction horizon are chosen to reduce on-line computational requirements. The discretized version of the stability constraint of the form $V(x(t+\Delta)) \leq 0.99V(x(t))$ is incorporated in the optimization problem.

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, $N = (0.447$ Kmol/m^3, 393 K). At $t = 0.16$ min, when the process state is at

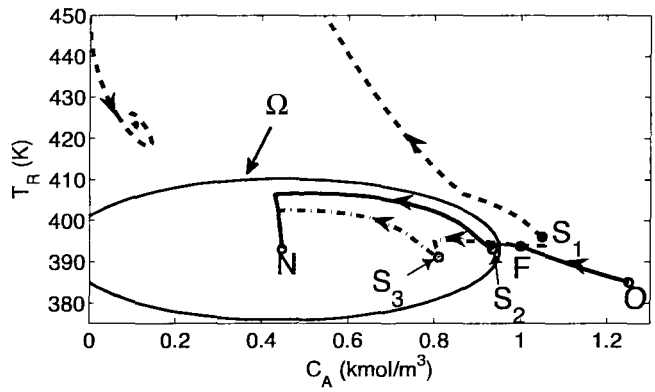


Figure 2.4: Evolution of closed-loop states for the CSTR example. Dashed line (- -) indicates the case when a safe-park point S_1 is arbitrarily chosen (resulting in the inability to resume nominal operation upon fault-recovery) while the solid line (—) indicates the case when S_2 is chosen according to Theorem 2.2, guaranteeing resumption of nominal operation upon fault-recovery. The dash-dotted lines show the closed-loop response when optimality considerations are included in the choice of the safe-park point and S_3 is chosen.

F = (0.9975 Kmol/m^3, 394.02 K), the heating valve fails, and reverts to the fail-safe position (completely shut) resulting in $Q_1 = 0$ KJ/s. This restricts the heat input/removal to -32 KJ/s $\leq Q < 0$ KJ/s instead of -32 KJ/s $\leq Q < 32$ KJ/s. A discrete manifold of available candidate safe-park points is generated by solving steady state system equations for allowable values of manipulated variables in faulty scenario. A grid of manipulated variables with interval of 0.0667 Kmol/m^3 and 0.1 KJ/s is used to generate the manifold of available candidate safe-park points. We first consider the case where the safe-park candidate S_1 is arbitrarily chosen as the safe-park point, and the process is stabilized at S_1 until the fault is rectified. At $t = 8.0$ min, the fault is rectified, however, we see that even after fault-recovery, nominal operation cannot be resumed (see dashed lines in Fig.2.4). This happens because S_1 lies outside the stability region under nominal operation. In contrast, if S_2 is chosen as the safe-park point, we see that the process can be successfully driven to S_2 with limited control

action as well as it can be successfully driven back to N after fault-recovery (see solid lines in Fig.2.4). The state and input profiles are shown in Fig.2.5. In summary, the simulation scenario illustrates the necessity to account for the presence of input constraints (characterized via the stability region) in the choice of the safe-park point.

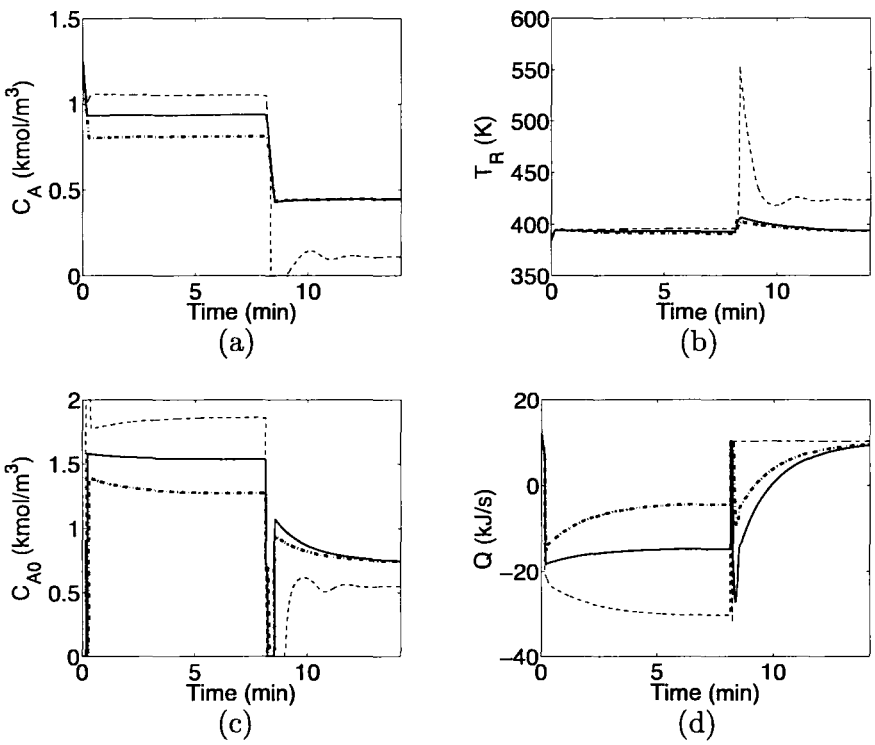


Figure 2.5: Evolution of the closed–loop state (a-b) and input (c-d) profiles for the CSTR example. Fault occurs at 0.16 min and is rectified at 8.0 min. Dashed lines (- -) indicate the case when a safe-park point S_1 is arbitrarily chosen (resulting in the inability to resume nominal operation upon fault-recovery) while the solid lines (—) show the case when S_2 is chosen according to Theorem 2.2, guaranteeing resumption of nominal operation upon fault-recovery. The dash-dotted lines show the closed–loop response when optimality considerations are included in the choice of the safe-park point and S_3 is chosen.

Next, we demonstrate the incorporation of performance criterion in selecting the safe-park point. To this end, we consider another point S_3 (corresponding to $Q_2 =$

-14.6 KJ/s, $C_{A0} = 1.53$ Kmol/m^3), which is also inside the stability region of N, and is thereby also a viable safe-park point (i.e., either of S_2 or S_3 can be chosen as safe-park point from stability perspective). Using the approach in Section 2.3.3, the cost associated with operating at the two safe-park points is calculated utilizing $f(x_s, u_s) = \|x^u_{ss}\|_{Q^2_s} + \|u_{ss}\|_{R^2_s}$ and the weighting matrices in Eqs. (2.26)-(2.28) are chosen as $Q_{tr} = Q_r = Q_s = \begin{bmatrix} 727 & 0 \\ 0 & 10 \end{bmatrix}$ and $R_{tr} = R_r = R_s = \begin{bmatrix} 0.64 & 0 \\ 0 & 0.04 \end{bmatrix}$. At the time of the failure, the auxiliary controller of Eq.2.20 is used to estimate J_{tr} and J_r, which are divided by T_s and T_r, to determine $J_{safe-parking} = \frac{J_{tr}}{T_s} + J_s + \frac{J_r}{T_r}$. Note that the fact that transition costs are divided by transition times implies that the computation of $J_{safe-parking}$ does not require prior information about the time of fault recovery. We also note that while in this illustrative simulation example, we only use two safe-park points for the purpose of illustration, the cost comparison can be carried out over a larger number of safe-park points (see the styrene process in Section 2.4). As the failure in the first actuator occurs when process is at point O (which is not the nominal operating point), the choice of optimal safe-park point needs to be made on-line. To reduce online compuational requirement for calculating cost $J_{safe-parking}$, we use the bounded controller get rough estimate for $J_{safe-parking}$. Table 2.4 shows the objective function value for the safe-park points calculated using the auxiliary controller. As can be seen from the table, the cost estimate for S_3 is significantly lower than for S_2, indicating that S_3 is a better choice for safe-parking the process. Subsequently, if S_3 is chosen as the safe-park point, it yields a closed–loop cost significantly lower than the closed–loop cost achieved when safe-parking the process at S_2 (the corresponding closed–loop state and input profiles are shown by the dash-dotted lines in Figs.2.4–2.5).

Table 2.4: Safe-parking cost estimates for the illustrative CSTR example of Section 2.3.4.

	C_A	T	**Objective function** $= J_{tr} + J_s + J_r$	
			Estimated using the bounded controller	**Closed–loop process cost**
S_2	0.9346	393	2406	4072
S_3	0.8107	391	1209	1105

2.4 Application to the styrene polymerization process

In this section, we implement the proposed safe-parking framework on the styrene polymerization process described in Section 2.2.7. To evaluate the robustness of the proposed framework, 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 flowrate F_i of magnitude 10% around the nominal values. The control objective is to stabilize the process at the nominal equilibrium point ($C_I = 0.067$ kmol/m^3, $C_M = 3.968$ kmol/m^3, $T = 303.55$ K, $T_c = 297.95$ K), corresponding to the nominal values of the manipulated inputs of $F_c = 0.131$ L/s and $F_m = 0.105$ L/s, while handling a fault in the valve manipulating the coolant flow rate.

For nominal operation, the predictive controller of Eqs.2.15–2.19 is designed using a quadratic control Lyapunov function of the form $V(x) = x'Px$. The matix

$P = \begin{bmatrix} 3662.2 & 89.43 & -18.59 & -25.02 \\ 89.430 & 2.953 & -0.628 & -0.845 \\ -18.592 & -0.628 & 0.682 & -0.036 \\ -25.023 & -0.845 & -0.036 & 2.002 \end{bmatrix}$ is generated by solving Riccati equation of Eq. 2.2. In Section 2.3.4 we demonstrated the implementation of the safe-parking framework where the fault occurs before the process is stabilized at the nominal equilibrium point. In this section we consider faults that occur after the process has been stabilized at the nominal equilibrium point. Determination of the safe-park points and evaluation of the cost estimates for safe-park points can therefore be carried out off-line. The nominal operating point for the process is a stable operating point, and several safe-park points satisfy the requirements of Theorem 2.2 (guaranteeing resumption of nominal operation upon fault-recovery). Ten safe-park points are chosen to be evaluated for optimality and using the approach in Section 2.3.3, the cost associated with each safe-park point is estimated using the cost function, $f(x_s, u_s) = \|u_{ss}\|_{R_s^2} - q_s M_{used}$, where the first term represents the cost of the utilities, while the second term represents the value of the product formed (via computing the rate of consumption of the monomer). With such a formulation of the steady-state cost, the safe-park points where the rate of product formation is more are preferred. The weighting factors are chosen as $R_s = \begin{bmatrix} 0.25 & 0 \\ 0 & 0 \end{bmatrix}$ and $q_s = 0.5$. The weighting matrices in Eqs.2.26-2.28 are chosen as diagonal matrices with the elements on the diagonal as $Q_{tr} = Q_r = diag(1000,\ 1000,\ 10,\ 10)$ and $R_{tr} = R_r = diag(1,\ 1)$.

For the safe-park points, the costs are calculated using the auxiliary controller of Eqs. 2.20-2.21 and tabulated in Table 2.5. Note that the cost is the minimum for the nominal operating point (with $J_{tr} = J_r = 0$), and out of the ten safe-park

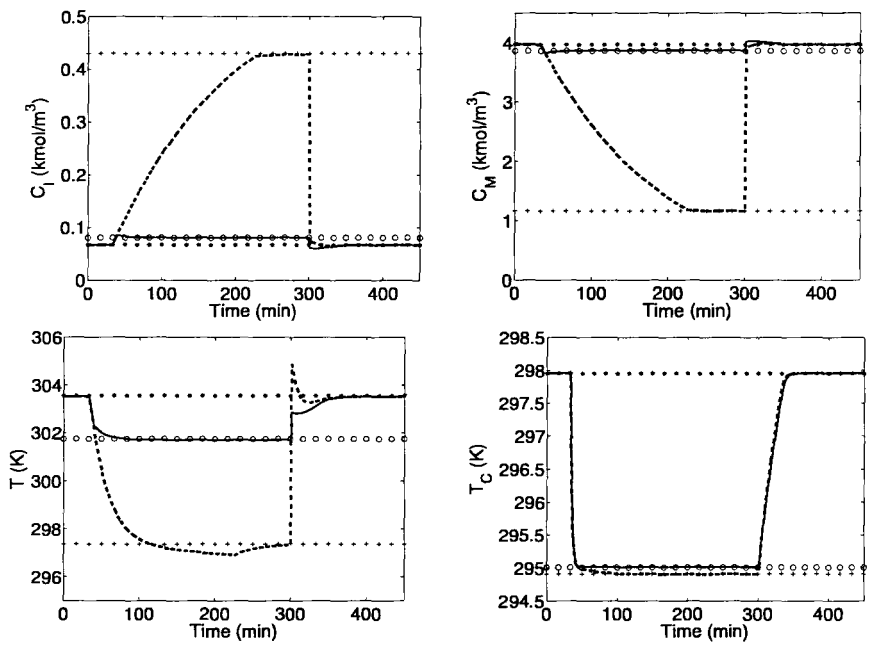


Figure 2.6: Evolution of the state profiles for the styrene polymerization process for an arbitrarily chosen safe-park point (dashed lines) and under the proposed safe-park mechanism (solid lines). Fault occurs at 33.3 min and is rectified at 300 min. The nominal equilibrium point N and the safe-park points S_5 and S_1 are denoted by the markers $\star$, o and $+$, respectively.

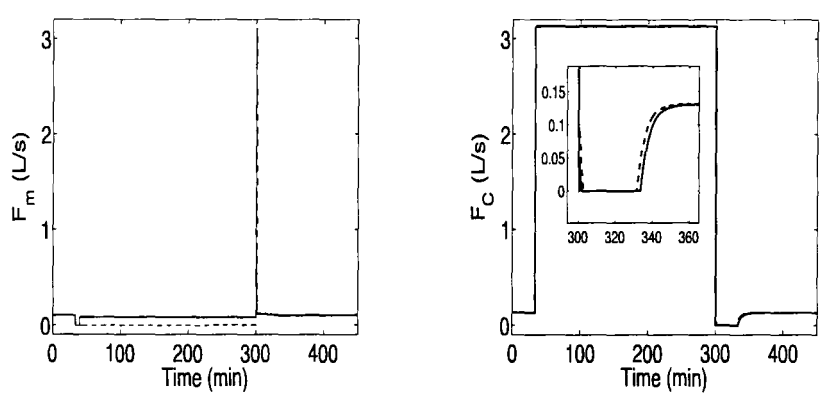


Figure 2.7: The input profiles for the styrene polymerization process for an arbitrarily chosen safe-park point (dashed lines) and under the proposed safe-park mechanism (solid lines). Fault occurs at 33.3 min, resulting in the coolant flow rate being stuck at the maximum value during this time, and is rectified at 300 min.

points, point S_5 ($C_I = 0.081$ kmol/m^3, $C_M = 3.863$ kmol/m^3, $T = 301.75$ K, $T_c = 295.01$ K) yields the lowest cost and and is therefore picked as the optimal safe-park point. Closed–loop simulations are shown for the case where a fault occurs at 33.3 minutes and is rectified at 300 mins. We first consider a case when S_1 ($C_I = 0.430$ kmol/m^3, $C_M = 1.165$ kmol/m^3, $T = 297.37$ K, $T_c = 294.91$ K) is picked as the safe-park point using the safe-parking framework (without considering performance criteria) and the closed–loop trajectories and input profiles are shown by the dashed line in Figs.2.6–2.7. Next, we use performance costs in Table 2.5 to select the optimal safe-park point (i.e. S_5). The closed–loop trajectories and input profiles are shown by the solid lines in Figs.2.6–2.7 when the safe-park point S_5 is picked. The closed–loop costs for the two points is also shown in Table 2.5. Once again, even in the presence of uncertainty and disturbances, the closed–loop costs follow the same trend as the estimates, yielding a low cost for the 'optimal' safe park point and demonstrating the robustness of the proposed safe-parking framework.

2.5 Conclusions

This chapter considered the problem of control of nonlinear process systems subject to input constraints and faults in the control actuators. A safe-parking framework was developed for handling faults that preclude the possibility of continued operating at the nominal equilibrium point. First, Lyapunov-based model predictive controllers, that allow for an explicit characterization of the stability region subject to constraints on the manipulated input, were designed. The stability region was utilized in selecting 'safe-park' points from the safe-park candidates (equilibrium points subject to failed actuators). Specifically, a candidate parking point was termed a safe-park point if

Table 2.5: Safe-parking cost estimates for the styrene polymerization process of Section 2.4.

	C_I	C_M	T	T_c	**Objective function** $= J_{tr} + J_s + J_r$	
					Bounded controller	**Closed-loop process cost**
N	0.0673	3.9685	303.5564	297.9532	-11.272	-
S_1	0.4298	1.165	297.3679	294.9115	-2.079	-2.144
S_2	0.2068	2.8708	299.2592	294.9543	-8.282	-
S_3	0.1362	3.4256	300.3554	294.9791	-9.407	-
S_4	0.1015	3.6998	301.1423	294.9969	-9.692	-
S_5	0.0809	3.8631	301.7465	295.0105	-9.734	-9.732
S_6	0.0673	3.9716	302.2279	295.0214	-9.655	-
S_7	0.0576	4.0488	302.6216	295.0303	-9.530	-
S_8	0.0503	4.1065	302.95	295.0378	-9.383	-
S_9	0.0447	4.1513	303.2285	295.0441	-9.227	-
S_{10}	0.0402	4.1871	303.4676	295.0495	-9.069	-
S_{11}	0.0365	4.2163	303.6754	295.0542	-8.912	-

1) the process state at the time of failure resides in the stability region of the safe-park candidate (subject to depleted control action), and 2) the safe-park candidate resides within the stability region of the nominal control configuration. Performance considerations, such as ease of transition from and to the safe-park point and cost of running the process at the safe-park point, were then quantified and utilized in choosing the optimal safe-park point. The proposed framework was illustrated using a chemical reactor example and its robustness with respect to parametric uncertainty and disturbances was demonstrated via a styrene polymerization process.

Bibliography

Ashraf Al-ghazzawi, Emad Ali, and Adnan Nouh. On-line tuning strategy for model predictive controllers. *Journal of Process Control*, 11:265–284, 2001.

S. Aumi and P. Mhaskar. Safe-steering of batch processes. *AIChE J.*, 55:2861–2872, 2009.

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

C. Chen and L. Shaw. On receding horizon feedback control. *Automatica*, 18(3): 349–352, 1982.

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.

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.

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

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

P. Dorato, C. T. Abdalla, and V. Cerone. *Linear Quadratic Control: An Introduction.* Krieger Pub Co, 2000.

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

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

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.

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.

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.

N. Huynh and N. Kazantzis. Parametric optimization of digitally controlled nonlinear reactor dynamics using zubov-like functional equations. *J. Math. Chem.*, 38:499–519, 2005.

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

C. Kravaris and S. Palanki. Robust nonlinear state feedback under structured uncertainty. *AIChE J.*, 34:1119–1127, 1988.

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

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

D. Q. Mayne and H. Michalska. Receding horizon control of nonlinear systems. *IEEE Trans. Automat. Contr.*, 35:814–824, 1990.

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.

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

P. Mhaskar. Robust model predictive control design for fault-tolerant control of process systems. *Ind. & Eng. Chem. Res.*, 45:8565–8574, 2006.

P. Mhaskar, N. H. El-Farra, and P. D. Christofides. Robust hybrid predictive control of nonlinear systems. *Automatica*, 41:209–217, 2005a.

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, 2005b.

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.*, 55:650–659, 2006a.

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, 2006b.

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.

H. Michalska and F. Mayne. Robust receding horizon control of constrained nonlinear systems. *IEEE Trans. on automatic Control*, 38:1512–1516, 1993.

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

Vesna Nevistí, James A. Primbs, and John C. Doyle. Nonlinear optimal control: A control lyapunov function and receding horizon perspective. *Asian Journal of Control*, 1:14–24, 1999.

Giuseppe De Nicolao, Lalo Magni, and Riccardo Scattolini. Stability and robustness of nonlinear receding-horizon control. In Alex Zheng Frank Allgwer, editor, *Progess in Systems and Control Theory: Nonlinear model predictive control*, volume 26, pages 3–22. Birkhäuser, 1999.

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.

S. J. Qin and T. J. Badgwell. An overview of nonlinear model predictive control applications. *Presented at Nonlinear MPC Workshop. Ascona, Switzerland*, 1998.

A. C. Raich and A. Cinar. Multivariate statistical methods for monitoring continuous processes: Assessment of discrimination power of disturbance models and diagnosis of multiple disturbances. *Chemom. & Int. Lab. Sys.*, 30:37–48, 1995.

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

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.

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

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.

T. Yang and E. Polak. Moving horizon control of nonlinear systems with input saturation, disturbances and plant uncertainty. *Int. J. Contr.*, 58:875–903, 1993.

S. Y. Yoon and J. F. MacGregor. Fault diagnosis with multivariate statistical models part I: using steady state fault signatures. *J. Proc. Contr.*, 11:387–400, 2001.

X. D. Zhang, T. Parisini, and M. M. Polycarpou. Adaptive fault-tolerant control of nonlinear uncertain systems: An information-based diagnostic approach. *IEEE Trans. Automat. Contr.*, 49:1259–1274, 2004.

Blank Page

Chapter 3

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

3.1 Introduction

In Chapter 2, a 'safe-parking' framework was developed that preserves process safety and enables smooth resumption of nominal operation on fault recovery via identifying appropriate 'safe-park' points where the process is stabilized during failure. The safe-parking framework in Chapter 2 assumes availability of the entire state information as well as precise process dynamics knowledge. However, in chemical process industries, all state are rarely measured and dynamics of unit processes/operations is difficult to model accurately. This requires that the control system design must account for estimation error associated with state estimation and also the plant-model mismatch.

*The results in this chapter are published in "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".

In addition to it, the control system also should be able to efficiently deal with process disturbances and measurement noise, which are ubiquitous in process industries. These requirements have motivated numerous research studies in the field of robust predictive controller designs to handle uncertainties in plant models, disturbances and measurement noise. Bemporad and Morari [1999] provides excellent survey on various robust model predictive controller designs and Mayne et al. [2000] analyzes stability and optimality of robust predictive controller for linear systems. For nonlinear systems, the problem of robust MPC design is still an area of ongoing research with significant number of research paper publishing every year (see, for example Michalska and Mayne [1993], Sarimveis et al. [1996], Magni et al. [2003], Wan and Kothare [2003], Langson et al. [2004], Wang and Rawlings [2004], Sakizlis et al. [2004], Mhaskar [2006], Mhaskar and Kennedy [2008], Mhaskar et al. [2007]). In robust predictive controllers, various design procedures achieve robust stability in two different ways: indirectly by specifying the performance objective and uncertainty description in such a way that the optimal control computation leads to robust stability; or directly by enforcing a type of robust contraction constraint which guarantees that the state will shrink for all plants in the uncertainty set (Bemporad and Morari [1999]). Several robust model predictive formulations utilize the "min-max" approach where the manipulated variables are calculated by solving as optimization problem that requires minimizing objective function over all possible realizations of the uncertainty. Robust predictive formulation in Zheng and Morari [1993] achieves robust stability by forcing the states to contract for all possible realization of uncertainties.

Lack of complete state measurements have also motivated plethora of research papers in field of state estimation, with most of research focusing on linear systems.

Since the optimal estimator generally is not available for the nonlinear systems, the estimator for nonlinear systems are based on sub-optimal approaches (Henson and Seborg [1997]). The high-gain observer proposed in Esfandiari and Khalil [1992] guarantees asymptotic stability of closed loop system and provides a handle on the decay rate of the estimation error by tuning observer gain (see Khalil [1992] for more details on high-gain observer).

As mentioned earlier, the safe-parking framework of Chapter 2 assumed 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-recovery.

Motivated by the above considerations, 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-recovery. 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 3.2.4. In Section 3.3.1 we extend the results in Mahmood and Mhaskar [2008] 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, present a polystyrene process example to motivate the proposed framework and formalize the control problem.

3.2.1 Process description

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

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

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. The vector function $f(x)$ and the matrices W, $G(x) = [g^1(x) \cdots g^m(x)]$ where $g^i(x) \in \mathbb{R}^n$, $i = 1 \cdots m$ are assumed to be sufficiently smooth on their domains of definition. Throughout the chapter, we assume that for any $u \in \mathbf{U}_\sigma$ the solution of the system of Eq.3.1 exists and is continuous for all t.

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 Hidalgo and Brosilow [1990] (also studied in, e.g., Prasad et al. [2002], Mahmood and Mhaskar [2008] and Chapter 2, 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)

$$
\begin{aligned}
\dot{C}_I &= \frac{(F_i C_{If} - F_t C_I)}{V_{pr}} - k_d C_I \\
\dot{C}_M &= \frac{(F_m C_{Mf} - F_t C_M)}{V_{pr}} - k_p C_M C_P \\
\dot{T} &= \frac{F_t(T_f - T)}{V_{pr}} + \frac{(-\Delta H)}{\rho c_p} k_p C_M C_P - \frac{hA}{\rho c_p V}(T - T_c) \\
\dot{T}_c &= \frac{F_c(T_{cf} - T_c)}{V_c} + \frac{hA}{\rho_c c_{pc} V_c}(T - T_c)
\end{aligned}
$$

$$\begin{aligned} C_P &= \left[\frac{2fk_dC_I}{k_t}\right]^{\frac{1}{2}} \\ k_d &= A_d e^{\frac{-E_d}{RT}} \\ k_p &= A_p e^{\frac{-E_p}{RT}} \\ k_t &= A_t e^{\frac{-E_t}{RT}} \end{aligned} \tag{3.2}$$

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 (Hidalgo and Brosilow [1990]), 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 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-recovery, 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 High gain observer

Here we briefly review the theory of high gain observer that will be used in Section 3.4 for estimating unmeasured states. There is no general procedure for designing state observer for nonlinear systems but some nonlinear systems, the design of such observer could be an easy as in linear systems. Consider a two dimensional system in the canonical form:

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= \phi(x,u) \\ y &= x_1 \end{aligned} \tag{3.3}$$

For this system a high gain observer can be designed as,

$$\begin{aligned} \dot{\hat{x}}_1 &= \hat{x}_2 + h_1(y - \hat{x}_1) \\ \dot{\hat{x}}_2 &= \phi_o(\hat{x},u) + h_2(y - \hat{x}_1) \end{aligned} \tag{3.4}$$

where $\phi_o(x,u)$ is a nominal model of $\phi(x,u)$. The dynamics of the estimation

error can be written as,

$$\begin{aligned} \dot{e}_1 &= -h_1 e_1 + e_2 \\ \dot{e}_2 &= -h_2 e_1 + \delta(x, e) \end{aligned} \tag{3.5}$$

where $x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, $x = \begin{bmatrix} x_1 - \hat{x}_1 \\ x_2 - \hat{x}_2 \end{bmatrix}$ and $\delta(x, e) = \phi(x, u) - \phi_o(\hat{x}, u)$

If there is no model-plant mismatch term, i.e. $\delta(x, e) = 0$, then asymptotic convergence of estimate is achieved by choosing h_1 and h_2 such that $A = \begin{bmatrix} -h_1 & 1 \\ -h_2 & 0 \end{bmatrix}$ is Hurwitz.

In presence of $\delta(x, u)$, it can be shown that by choosing $h_2 \ll h_1 \ll 1$, specifically by taking $h_1 = \frac{\alpha_1}{\epsilon}$, $h_1 = \frac{\alpha_2}{\epsilon^2}$ for some positive constant α_1, α_2 and ϵ with $\epsilon \ll 1$, the effect of $\delta(x, u)$ on estimation error diminishes. For example, if the system in Eq. 3.3 is second order, then the transfer function from δ to e is given by,

$$\begin{aligned} G_o(s) =& \frac{1}{s^2 + h_1 s + h_2} \begin{bmatrix} 1 \\ s + h_1 \end{bmatrix} \\ =& \frac{\epsilon}{(\epsilon s)^2 + \alpha_1 \epsilon s + \alpha_2} \begin{bmatrix} \epsilon \\ \epsilon s + \alpha_1 \end{bmatrix} \end{aligned} \tag{3.6}$$

Thus $\lim_{\epsilon \to 0} G_o(s) = 0$. As mentioned earlier, reducing ϵ, diminishes the effect of δ on estimation error but it should be noted that it also gives rise to peaking phenomenon, where error (e) exhibits an impulsive like behavior where transient peaks to $O(1/\epsilon)$ value before it decays rapidly towards zero (see Khalil [1992] for more details on high-gain observer).

3.2.4 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 w.l.o.g., in the first control actuator at a time T^{fault}, subsequently rectified at a time $T^{recovery}$ (i.e., for $t \leq T^{fault}$ and $t > T^{recovery}$, $\sigma(t) = 1$ and $\sigma(t) = 2$ for $T^{fault} < t \leq T^{recovery}$), as $u_2^1(t) = u_{failed}^1$, with $u_{min,2}^1 \leq u_{failed}^1 \leq u_{max,2}^1$, where u^i denotes the ith component of a vector u, for all $T^{fault} < t \leq T^{recovery}$, 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 $u_{failed}^1 \neq 0$, then it may happen that $0 \notin X_c$, i.e., if the failed actuator is frozen at a non-nominal value, then it is possible that the process simply cannot be stabilized at the nominal equilibrium point using the functioning control actuators. 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-recovery. 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-recovery 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 Mahmood and Mhaskar [2008], as well as the the safe-parking framework of Chapter 2. 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. Preparatory to the presentation of the robust predictive controller for the system of Eq.3.1, we define the set (in line with

the idea of Section 2.2.3):

$$\Pi = \{x \in \mathbb{R}^n : L_f V(x) + \sum_{i=1}^{q} L_{W_i}^{max} V(x)\theta^i + \sum_{i=1}^{m} L_{G_i}^{min} V(x)u^i + \rho V(x) \leq 0\} \quad (3.7)$$

where $L_{W_i}^{max} V(x)\theta^i = L_{W_i} V(x)\theta_{min}^i$, if $L_{W_i} V(x) \leq 0$ and $L_{W_i}^{max} V(x)\theta^i = L_{W_i} V(x)\theta_{max}^i$, if $L_{W_i} V(x) > 0$ and $L_{G_i}^{min} V(x)u^i = L_{G_i} V(x)u_{max}^i$, if $L_{G_i} V(x) \leq 0$ and $L_{G_i}^{min} V(x)u^i = L_{G_i} V(x)u_{min}^i$, if $L_{G_i} V(x) > 0$ (for a discussion on the definition of the set Π, see Section 2.2.3 and Remark 3.1) and assume that $\Omega := \{x \in \mathbb{R}^n : V(x) \leq c^{max}\} \subseteq \Pi$ for some $c^{max} > 0$ (see Section 2.2.3 for more details). Consider now the receding horizon implementation of the control action computed by solving an optimization problem of the form:

$$u_{MPC}(x) := \arg min\{J(x, t, u(\cdot))|u(\cdot) \in S\} \quad (3.8)$$

$$s.t. \ \dot{x} = f(x) + G(x)u \quad (3.9)$$

$$L_G V(x)u \leq -L_f V(x) - \sum_{i=1}^{q} L_{W_i}^{max} V(x)\theta^i - \rho V(x) \quad (3.10)$$

$$x(\tau) \in \Pi \ \forall \ \tau \in [t, t + \Delta) \quad (3.11)$$

where $L_G V = [L_{g^1} V \ \cdots \ L_{g^m} V]$ is a row vector and 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 U. Eq.3.9 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

$$J(x, t, u(\cdot)) = \int_t^{t+T} \left[\|x^u(s; x, t)\|_Q^2 + \|u(s)\|_R^2 \right] ds \tag{3.12}$$

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.3.9, 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 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.3.8–3.12. 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.3.8-3.12 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.3.8-3.12 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.3.8-3.12 (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.3.8-3.12, 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.3.10 for feasibility. Since $\Omega \in \Pi$ and $x_0 \in \Omega$, this implies that there exists a $u^* \in S$ such that $L_G V(x)u(t) \leq -L_f V(x) - \sum_{i=1}^{q} L_{W_i^{max}} V(x)\theta^i - \rho V(x)$. 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.3.10.

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.3.8-3.12 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.3.8-3.12 (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.3.10 implies that for all $x(0) \in \Omega$ and $\|\theta(t)\| \leq \theta_b$

$$\begin{aligned} \dot{V}(x) &= L_f V + L_G V u + L_W V \theta(t) \\ &\leq -\rho V(x) \end{aligned} \tag{3.13}$$

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, $\forall \; t \in [0, \Delta^{**}]$,

$$\begin{aligned} \dot{V}(x(t)) &= L_f V(x(t)) + L_G V(x(t)) u_0 + L_W V(x(t)) \theta(t) \\ &= L_f V(x_0) + L_G V(x_0) u_0 + L_W V(x_0) \theta(0) + (L_f V(x(t)) - L_f V(x_0)) \\ &\quad + (L_G V(x(t)) u_0 - L_G V(x_0) u_0) + L_W V(x(t)) \theta(t) - L_W V(x_0) \theta(0) \end{aligned} \tag{3.14}$$

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 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 $\|L_f V(x(t)) - L_f V(x_0)\| \leq K^3 K^1 \Delta^{**}$, $\|L_G V(x(t)) u_0 - L_G V(x_0) u_0\| \leq K^2 K^1 \Delta^{**}$ and $\|L_W V(x(t)) \theta(t) - L_W V(x_0) \theta(0)\| \leq K^4 K^1 \Delta^{**}$. Using these inequalities in Eq.3.14, we get

$$\dot{V}(x(t)) \leq -\rho(c^{max} - \delta) + (K^1 K^2 + K^1 K^3 + K^1 K^4) \Delta^{**} \tag{3.15}$$

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

$$\epsilon < \rho(c^{max} - \delta) \tag{3.16}$$

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

$$\delta' = \max_{V(x_0) \leq c^{max} - \delta,\, u \in \mathcal{U},\, \theta \in \Theta\; t \in [0, \Delta']} V(x(t)) \tag{3.17}$$

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.3.17 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 $x_0 \in \Pi \notin \Omega$. 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.3.10 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. The inclusion of uncertainty term in the

characterization of the stability region results in contraction of the stability region as compared to the stability region for the system without uncertainty. In Fig. 3.1, the contraction of the stability region is shown. The degree of the contraction depends on the magnitude of the uncertainty considered, the equilibrium point and inherent robustness of the system.

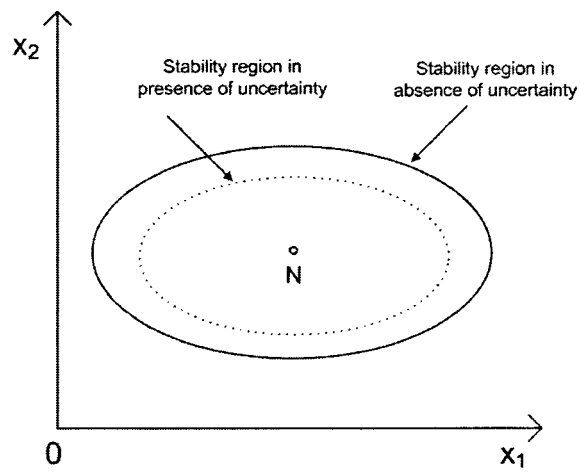


Figure 3.1: Schematic for stability region characterization in the presence of uncertainty. Inclusion of the uncertainty term in the characterization of stability region results in contraction of the stability region as compared to the stability region for the system without uncertainty term.

Remark 3.2. 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 Mhaskar [2006] uses an auxiliary control

law in formulating the robust stability constraint and the stability region of the robust predictive controller of Mhaskar [2006] is limited to the (possibly conservative) stability region estimate of the auxiliary control law. More recently, a Lyapunov-based controller is proposed (Mahmood and Mhaskar [2008]) that enhances the set of initial conditions from where closed–loop stability is achieved compared to Lyapunov-based bounded control designs. The predictive controller of Mahmood and Mhaskar [2008] however, 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.

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 $u_{MPC}(x + e)$. 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.3.8-3.12 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 $\limsup_{t\to\infty} \|x(t)\| \leq d$.

Remark 3.3. 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 for its subsequent use within the output feedback predictive controller in Section 3.4.1.

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 $T^{recovery}$, and for which the robust stability region under nominal operation, denoted by Ω_n, has been characterized using the predictive controller formulation of Eqs.3.8–3.12. 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.3.8–3.12, 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.3.8-3.12. If* $x(0) \in \Omega_n$, $x(T^{fault}) \in \Omega_c$ *and* $\Omega_c \subset \Omega_n$, *then the switching rule*

$$u(t) = \left\{ \begin{array}{lll} u_{1,n} & , & 0 \leq t < T^{fault} \\ u_{2,x_c} & , & T^{fault} \leq t < T^{recovery} \\ u_{1,n} & , & T^{recovery} \leq t \end{array} \right\} \tag{3.18}$$

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 ($T^{fault} = T^{recovery} = \infty$), and second if a fault occurs at a time $T^{fault} < \infty$ and is recovered at a time $T^{fault} \leq T^{recovery} < \infty$.

Case 1: The absence of a fault implies $u(t) = u_{1,n} \; \forall \; t \geq 0$. Since $x(0) \in \Omega_n$, and the nominal control configuration is implemented for all times, we have from Theorem 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 $T^{recovery}$. Since $x(T^{fault}) \in \Omega_c \subset \Omega_n$, we have that $x(t) \in \Omega_n \; \forall \; T^{fault} \leq t \leq T^{recovery}$. At a time $T^{recovery}$, we therefore also have that $x(T^{recovery}) \in \Omega_n$. Subsequently, as with case 1, the nominal control configuration is implemented for all time thereafter, we have that $x(t) \in \Omega_n \; \forall \; t \geq T^{recovery}$. In conclusion, we have that $x(t) \in \Omega_n \; \forall \; t \geq 0$ and $\limsup_{t \to \infty} \|x(t)\| \leq d$. This completes the proof of Theorem 3.2.

Remark 3.4. 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-recovery. 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 Mhaskar [2006]) 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.

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:

$$\begin{aligned} \dot{C}_A &= \frac{F}{V}(C_{A,in} - C_A) - k_0 e^{\frac{-E}{RT_R}} C_A \\ \dot{C}_B &= \frac{F}{V}(C_{B,in} - C_B) + k_0 e^{\frac{-E}{RT_R}} C_A \\ \dot{T}_R &= \frac{F}{V}(T_{in} - T_R) + \frac{(-\Delta H)}{\rho_f c_p} k_0 e^{\frac{-E}{RT_R}} C_A + \frac{Q}{\rho_f c_p V} \end{aligned} \tag{3.19}$$

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 3.1. The control objective is to stabilize the reactor at the unstable equilibrium point $(C_A^s,\ T_R^s) = (0.45\ \text{Kmol/m}^3, 393\ \text{K})$ in the presence of uncertainty. Specifically, we consider an error in the parameter ΔH of magnitude 1%, a sinusoidal disturbance in the inlet temperature T_{in} of magnitude 10% around the nominal value, random disturbances in F, $C_{A,in}$ of magnitude 1% around the nominal value, and a random disturbance in Q of magnitude 5% around the nominal value. 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, $0\ \text{KJ/s} \leq Q_1 \leq 32\ \text{KJ/s}$ and $-32\ \text{KJ/s} \leq Q_2 \leq 0\ \text{KJ/s}$. 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 using grid search technique as described in Section 2.2.3 with grid interval of 0.6 °C and 0.004 Kmol/m^3. The stability region is denoted by Ω in Fig.3.2. 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 $-32\ \text{KJ/s} \leq Q_2 <$

Table 3.1: Chemical reactor parameters and steady–state values.

V	=	0.1	m^3
R	=	8.314	KJ/(Kmol · K)
C_{A,in_s}	=	0.73	Kmol/m^3
T_{in_s}	=	310.0	K
Q_s	=	10.0	KJ/s
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 · 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

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. 3.12), 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. It should be noted that as the stability of closed loop process system is guaranteed by use of the stability constraint in the controller formulations,

short prediction horizon are chosen to reduce on-line computational requirements.

Consider a scenario where the process starts from $O = (1.25\ \text{Kmol/m}^3,\ 385\ \text{K})$ and the predictive controller drives the process toward the nominal operating point, N. At $t = 0.5$ min, when the process state is at $F = (1\ \text{Kmol/m}^3,\ 393.76\ \text{K})$, 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 $-32\ \text{KJ/s} \leq Q < 0\ \text{KJ/s}$ instead of $-32\ \text{KJ/s} \leq Q < 32\ \text{KJ/s}$.

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-recovery, nominal operation cannot be resumed (see dashed lines in Fig.3.2). This happens because S_1 lies outside the stability region under nominal operation. In contrast, if S_2 is chosen as the safe-park point, we see that the process can be successfully driven to S_2 with limited control action as well as it can be successfully driven back to N after fault-recovery (see solid lines in Fig.3.2). The state and input profiles are shown in Fig.3.3. 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

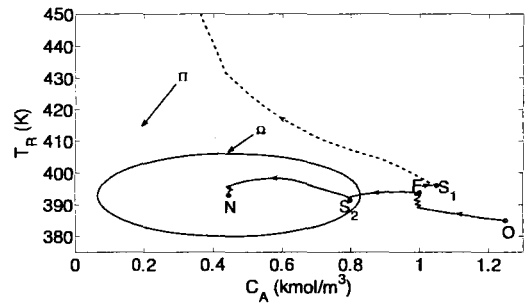


Figure 3.2: Evolution of the state trajectory for the CSTR example in the presence of uncertainty. Dashed line (- -) indicates the case when a safe-park point S_1 is arbitrarily chosen (resulting in the inability to resume nominal operation upon fault-recovery) while the solid line (—) indicates the case when S_2 is chosen according to Theorem 3.2, guaranteeing resumption of nominal operation upon fault-recovery.

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*

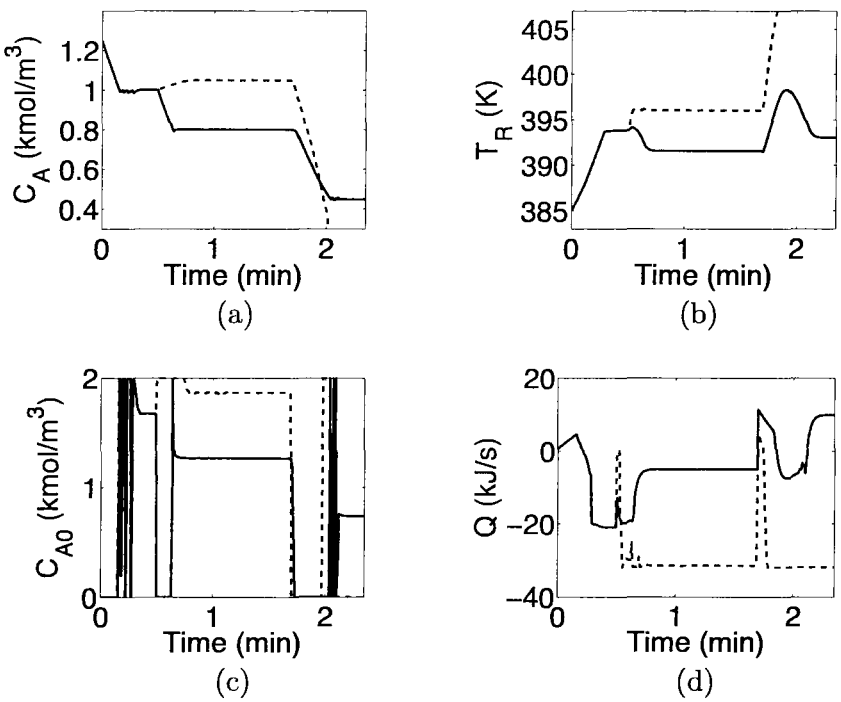


Figure 3.3: Evolution of the closed–loop state (a-b) and input (c-d) profiles for the CSTR example in the presence of uncertainty. Fault occurs at 0.5 min and is rectified at 1.7 min. Dashed lines (- -) indicate the case when a safe-park point S_1 is arbitrarily chosen (resulting in the inability to resume nominal operation upon fault-recovery) while the solid lines (—) show the case when S_2 is chosen according to Theorem 3.2, guaranteeing resumption of nominal operation upon fault-recovery.

$$\begin{aligned} \dot{\xi}_1^{(i)} &= \xi_2^{(i)} \\ &\vdots \\ \dot{\xi}_{r_i-1}^{(i)} &= \xi_{r_i}^{(i)} \\ \dot{\xi}_{r_i}^{(i)} &= L_f^{r_i} h_i(x) + \sum_{j=1}^{m} L_{g_j} L_f^{r_i-1} h_i(x) u_j \end{aligned} \tag{3.20}$$

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* $x \longrightarrow 0$. Preparatory 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. Note that Assumption 2 is satisfied for practically all chemical processes.

Assumption 2. Consider the nonlinear system of Eq.3.1 with $u \in U$. *Then, given any positive real numbers* $\delta > \delta_b$, *there exists a 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 Munoz de la Pena and Christofides [2008]). 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 3.1), 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.3.8–3.12:*

$$\dot{\tilde{y}}^{(i)} = \begin{bmatrix} -L_i a_1^{(i)} & 1 & 0 & \cdots & 0 \\ -L_i^2 a_2^{(i)} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -L_i^n a_r^{(i)} & 0 & 0 & \cdots & 0 \end{bmatrix} \tilde{y}_i + \begin{bmatrix} L_i a_1^{(i)} \\ L_i^2 a_2^{(i)} \\ \vdots \\ L_i^n a_n^{(i)} \end{bmatrix} y_m \tag{3.21}$$

$$u = u_{mpc}(\hat{x})$$

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 3.1.

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 $\tilde{b}_i$:

$$\tilde{A}_i = \begin{bmatrix} -a_1^{(i)} & 1 & 0 & \cdots & 0 \\ -a_2^{(i)} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_{r-1}^{(i)} & 0 & 0 & \ldots & 1 \\ -a_r^{(i)} & 0 & 0 & \cdots & 0 \end{bmatrix}, \tilde{b} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}, \tag{3.22}$$

the system of Eq.3.9 under the controller of Eq.3.21 takes the following form:

$$\varepsilon_i \dot{e}_o^{(i)} = \tilde{A}_i e_o^{(i)} + \varepsilon_i b \Psi(x, \hat{x}), i = 1, \ldots, m \tag{3.23}$$

$$\dot{x} = f(x) + g(x)u(\hat{x}) \tag{3.24}$$

where $\Psi(x, \hat{x})$ is a Lipschitiz function of its argument. Owing to the presence of the small parameter ε_i that multiplies the time derivative $\dot{e}_o^{(i)}$, the system of Eq.3.23 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:

$$\frac{de_o^{(i)}}{d\tau} = \tilde{A}_i e_o \tag{3.25}$$

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 3.1), 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 3.1 can be invoked to prove practical stability of the closed–loop system. This concludes the proof of Theorem 3.3.

Remark 3.5. 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.

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 3.1 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 Mhaskar et al. [2004] and El-Farra et al. [2005] in the context of hybrid predictive control of linear systems and nonlinear switched systems under output feedback. The proof of Proposition 3.1 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 3.1. 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.3.21 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.3.8–3.11. 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

$$u(t) = \left\{ \begin{array}{lll} u_{1,n} & , & 0 \leq t < T^{fault} \\ u_{2,x_c} & , & T^{fault} \leq t < T^{recovery} \\ u_{1,n} & , & T^{recovery} \leq t \end{array} \right\} \tag{3.26}$$

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 recovery, 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 3.6. 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 3.1 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 a fault takes place before the estimates have converged, the safe-parking decision can be delayed to achieve estimate convergence and allow for appropriate picking of the safe-park point (see simulation example in Section 3.4.3 for a demonstration).

Remark 3.7. Note that while 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. Chapter 4 presents safe-parking framework to handle faults in networked-plant setting. 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.

$$\begin{aligned} \dot{\tilde{y}}_1^{(1)} &= L_1 a_1^{(1)}(y_1 - \tilde{y}_1^{(1)}) \\ \dot{\tilde{y}}_1^{(2)} &= \tilde{y}_2^{(2)} + L_2 a_1^{(2)}(y_2 - \tilde{y}_1^{(2)}) \\ \dot{\tilde{y}}_2^{(2)} &= L_2^2 a_2^{(2)}(y_2 - \tilde{y}_1^{(2)}) \end{aligned} \tag{3.27}$$

The observer parameters in the state estimator design of Eq.3.27 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 $F = (0.99\ \text{Kmol/m}^3,\ 394.02\ \text{K})$ the observer is initialized at E = $(0.03\ \text{Kmol/m}^3,\ 424\ \text{K})$, and the predictive controller drives the process toward the nominal operating point, $N = (0.45\ \text{Kmol/m}^3,\ 393\ \text{K})$. 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 $S_1 = (0.17\ \text{Kmol/m}^3, 424.75\ \text{K})$ 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 $((0.8\ \text{Kmol/m}^3, 391.5\ \text{K}))$ is chosen as the safe-park point. Subsequently, the process is driven to and back from the safe park point after fault-recovery (see solid lines in Fig.3.4). The state and input profiles

are shown in Fig.3.5. 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.

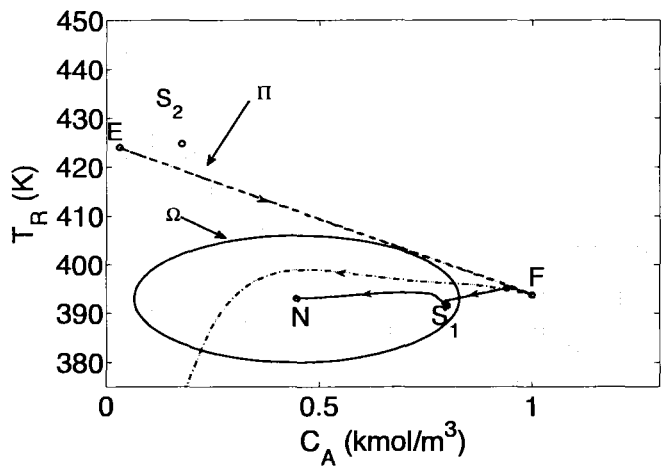


Figure 3.4: Evolution of closed–loop states and closed–loop state estimates for the CSTR example with limited availability of state measurements. The dashed–dot line (- .) and dotted line (...) represents the state estimates and state trajectories for the case when a safe-park point S_2 is immediately 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 3.3), guaranteeing stabilization at the safe-park point and subsequent resumption of nominal operation upon fault-recovery.

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

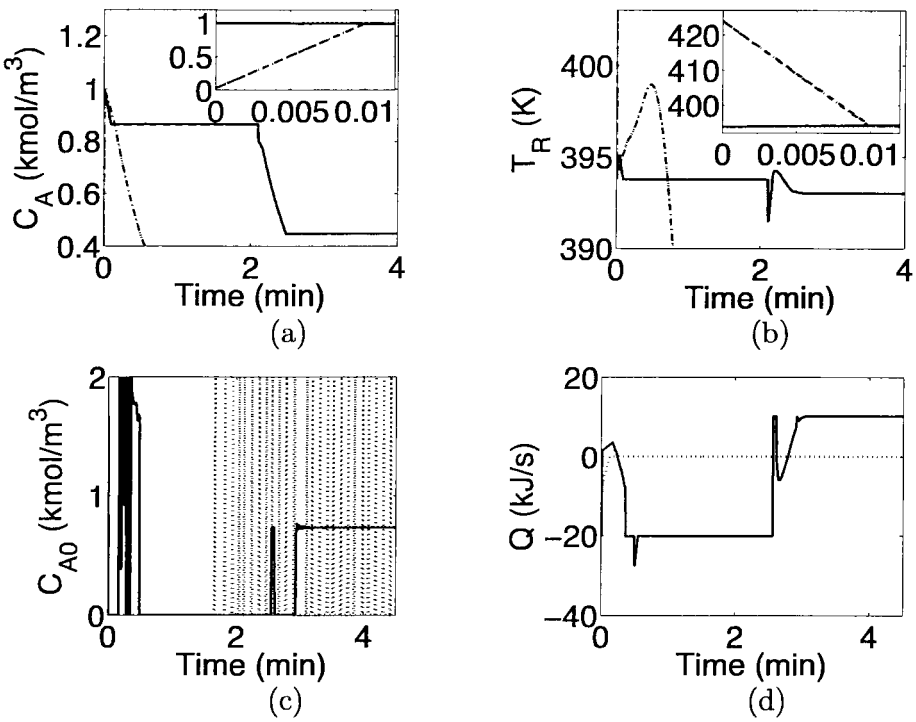


Figure 3.5: Evolution of the closed–loop state (a-b) and input (c-d) profiles for the CSTR example with limited availability of state measurements. Fault occurs at 0.05 min and is rectified at 2 min. The dashed–dot line (- .) and dotted line (...) represents the state estimates and state trajectories 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 3.4), guaranteeing stabilization at the safe-park point and subsequent resumption of nominal operation upon fault-recovery.

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 fluctuations in the initiator flowrate F_i and cooling water inlet temperature T_{cf} of magnitude 2% and 10%, respectively, around their nominal values. It is assumed that measurements are available only for C_M and T (with random measurement error of magnitude $\pm 5\%$ in C_M and ± 0.5 K in T). 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. 3.21 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.3.8–3.12 is designed using a quadratic Lyapunov function of the form $V(x) = x'Px$. The matrix $P = \begin{bmatrix} 2091.4 & 35.9537 & -6.5924 & 9.1116 \\ 35.9537 & 1.1603 & -0.2231 & 0.3084 \\ -6.5924 & -0.2231 & 0.8473 & -0.2857 \\ 9.1116 & 0.3084 & -0.2857 & 1.4576 \end{bmatrix}$ is generated by solving Riccati equation of Eq. 2.2.

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.3.6 (see Fig.3.7 for the corresponding manipulated input profiles), the observer converges to the true state values sufficiently fast and drives the process to the nominal equilibrium point.

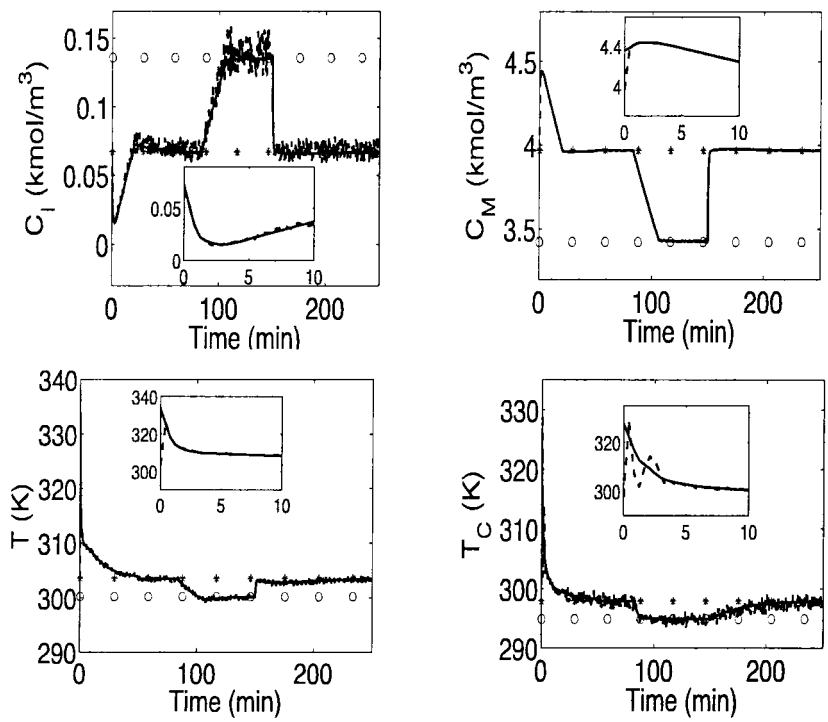


Figure 3.6: Evolution of the state (solid lines) and state estimates profiles (dashed lines) for the styrene polymerization process. Fault occurs at 83.3 min and is rectified at 150 min. The nominal equilibrium point N and the safe-park point S are denoted by the markers $\star$ and o, respectively.

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 $t = 83.3$ min, 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.

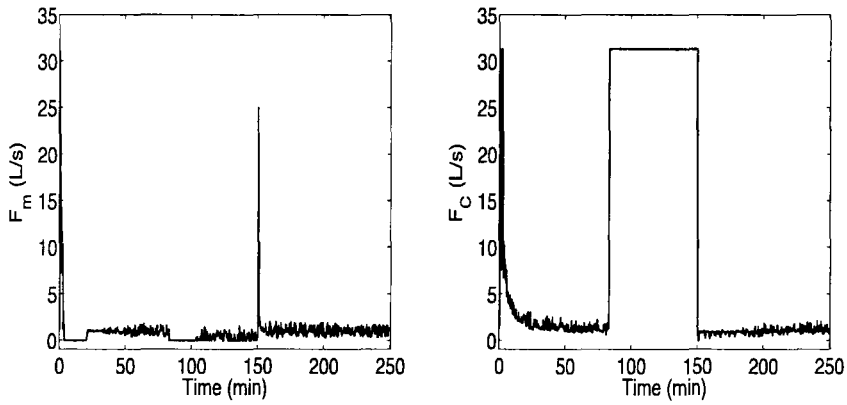


Figure 3.7: The input profiles for the styrene polymerization process. Fault occurs at 83.3 min and is rectified at 150 min. The nominal equilibrium point N and the safe-park point S are denoted by the markers $\star$ and o, respectively.

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 unavailability 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 the safe-parking algorithm that preserves closed–loop stability upon fault recovery. 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.

Bibliography

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.

A. Bemporad and M. Morari. Robust model predictive control: A survey. In : A. Garulli, A. Tesi and A. Vicino (Eds.), *Robustness in Identification and Control, Lecture Notes in Control and Information Sciences* Vol. 245, pages 207–266, Berlin: Springer, 1999.

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.

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.

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

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

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

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

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

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

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.

F. Esfandiari and H.K. Khalil. Output feedback stabilization of fully linearizable systems. *International Journal of Control*, 56(5):1007 – 1037, 1992.

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.

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.

M. A. Henson and D. E. Seborg. *Nonlinear Process Control.* Prentice-Hall, Englewood Cliffs, NJ, 1997.

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.

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

H. K. Khalil. *Nonlinear Systems.* Macmillan Publishing Company, New York, 1992.

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.

W. Langson, I. Chryssochoos, S. V. Rakovic, and D. Q. Mayne. Robust model predictive control using tubes. *Automatica*, 40:125–133, 2004.

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

L. Magni, G. Nicolao, R. Scattolini, and F. Allgower. Robust model predictive control for nonlinear discrete-time systems. *Int. J. Rob. & Non. Contr.*, 13:229–246, 2003.

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

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

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.

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

P. Mhaskar. Robust model predictive control design for fault-tolerant control of process systems. *Ind. & Eng. Chem. Res.*, 45:8565–8574, 2006.

P. Mhaskar and A. B. Kennedy. Robust model predictive control of nonlinear process systems: Handling rate constraints. *Chem. Eng. Sci.*, 63:366–375, 2008.

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

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.

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.*, 55:650–659, 2006a.

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, 2006b.

P. Mhaskar, N. H. El-Farra, and P. D. Christofides. Robust predictive control of switched systems: Satisfying uncertain schedules subject to state and control constraints. *Int. J. Adapt. Contr. & Sign. Process.*, 22:161–179, 2007.

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.

H. Michalska and D. Q. Mayne. Robust receding horizon control of constrained nonlinear systems. *IEEE Trans. Automat. Contr.*, 38:1623–1633, 1993.

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.

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

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

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.

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.

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

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.

V. Sakizlis, N. M. P. Kakalis, V. Dua, J. D. Perkins, and E. N. Pistikopoulos. Design of robust model–based controllers via parametric programming. *Automatica*, 40: 189–201, 2004.

H. Sarimveis, H. Genceli, and M. Nikolaou. Design of robust nonsquare constrained model-predictive control. *AIChE J.*, 42:2582–2593, 1996.

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

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.

Y. J. Wang and J. B. Rawlings. A new robust model predictive control method I: theory and computation. *J. Proc. Contr.*, 14:231–247, 2004.

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.

Z.Q. Zheng and M. Morari. Robust stability of constrained model predictive control. In *Proceedings of the 1993 American Control Conference (IEEE Cat. No.93CH3225-0)*, pages 379 – 383, Evanston, IL, USA, 1993.

Chapter 4

A Safe-Parking Framework for Plant-Wide Fault-Tolerant Control *

4.1 Introduction

In Chapter 2, a safe-parking framework is developed to address the problem of determining how to run an isolated unit during fault-rectification to prevent onset of hazardous situations and enable smooth transition to nominal operation upon fault repair. In Chapter 3, the safe-parking framework is extended to handle uncertainty and limited availability of measurements. The results in Chapter 2 and Chapter 3, however, consider safe-parking in the context of an isolated unit. The opportunities and challenges that arise in a plant-wide setting due to the connected nature of chemical processes via material, energy or communication lines simply do not exist in an isolated unit. The results in Chapter 2 and Chapter 3 therefore cannot be applied to a

*The results in this chapter are published in "R. Gandhi and P. Mhaskar, A safe-parking framework for plant-wide fault-tolerant control, *Chem. Eng. Sci.*, 64:3060-3071, 2009".

plant-wide setting. Infact, a simple application of the results in Chapter 2 and Chapter 3 to a multi-unit setting can result in missed opportunities as well as inadequate safe-parking. In particular, when safe-parking a unit in a plant, the fact that the outlets from the faulty unit go to another unit (where functioning manipulated inputs exist) can help in localizing the effect of the fault to the faulty unit, and preserving nominal operation in the downstream plant. On the other hand, if the fact that a unit (when multiple units are being safe-parked) receives altered (or non-nominal) outlet streams from an upstream safe-parked unit is not accounted for, it can result in the inability to adequately safe-park the unit in question. In particular, a change in operating condition of one unit naturally acts as a disturbance to the downstream units and hence large changes in operating conditions of one unit, while possibly enabling safe-parking of the unit in question, can jeopardize the operation of the downstream units, and therefore of the whole plant. This necessitates that the safe-park point for a unit in multi-unit processes be chosen with adequate consideration of its effect on downstream units.

Motivated by the above considerations, this chapter addresses the problem of handling faults in the context of multi-unit processes. We consider a multi-unit nonlinear process system subject to input constraints and actuator faults in one unit that preclude the possibility of operating the unit at its nominal equilibrium point. We first consider the case where there exists a safe-park point for the faulty unit such that its effect can be completely rejected (via changing the nominal values of the manipulated variables) in the downstream unit. Steady-state as well as dynamic considerations (including the presence of input constraints) are used in determining the necessary conditions for safe-parking the multi-unit system. We next consider

the problem where no viable safe-park point for the faulty unit exists such that its effect can be completely rejected in the subsequent unit. A methodology is developed that allows simultaneous safe-parking of the consecutive units. Finally, we incorporate performance considerations in the safe-parking framework for the multi-unit processes.

The rest of the chapter is organized as follows: First in Section 4.2.1, we present the class of processes considered. Next we review a Lyapunov-based predictive controller in Section 4.2.2 and safe-parking framework for an isolated unit in Section 4.2.3. In Section 4.3 we present the safe-parking framework for multi-unit processes, first presenting the case where a unit can be safe-parked to allow nominal operation in the subsequent unit in Section 4.3.2 and then presenting the methodology for simultaneous safe-parking in Section 4.3.3. The details of the framework are illustrated using a chemical process with two chemical reactors in Section 4.4, and we summarize our results in Section 4.5.

4.2 Preliminaries

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

4.2.1 Process description

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

$$\begin{aligned}
\dot{x}_1 &= f_1(x_1) + G_1(x_1)(u_1 + h_1) \\
\dot{x}_2 &= f_2(x_2) + G_2(x_2)(u_2 + h_2) + W_{2,1}(x_2)x_1 \\
&\vdots \\
\dot{x}_i &= f_i(x_i) + G_i(x_i)(u_i + h_i) + W_{i,i-1}(x_i)x_{i-1} \\
&\vdots
\end{aligned}$$

$$\dot{x}_M = f_M(x_M) + G_M(x_M)(u_M + h_M) + W_{M,M-1}(x_M)x_{M-1} \tag{4.1}$$

where $x_i := [x_i^1\ x_i^2 \cdots x_i^{n_i}]' \in \mathbb{R}^{n_i}$ $i \in [1,\ M]$ denotes the vector of state variables for the i^{th} unit and $u_i(t) := [u_i^1\ u_i^2 \cdots u_i^{m_i}] \in \mathbb{R}^{m_i}$ denotes the vector of constrained manipulated variables for the i^{th} unit, taking values in a nonempty convex subset $\mathbf{U_i}$ of $\mathbb{R}^{m_i}$, where $\mathbf{U_i} = \{u_i \in \mathbb{R}^{m_i} : u_{i,min} \leq u_i \leq u_{i,max}\}$, where $u_{i,min}, u_{i,max} \in \mathbb{R}^{m_i}$ denote the constraints on the manipulated variables of the i^{th} unit. $h_i(t) := [h_i^1\ h_i^2 \cdots h_i^{m_i}] \in \mathbb{R}^{m_i}$ is a vector that captures the effect of the actuator faults on the process states. $h_i^j = 0$ for $t < t_{i,f}^j$ and $t > t_{i,r}^j$; $h_i^j = -u_i^j + u_{i,failed}^j$ for $t_{i,f}^j \geq t \geq t_{i,r}^j$, where $t_{i,f}^j$ and $t_{i,r}^j$ denote the fault occurrence and recovery times and $u_{i,failed}^j$ denotes the fail-safe value for the j^{th} actuator in the i^{th} unit. The vector function $f_i(x_i)$ and the matrix functions $G_i(x_i) = [g_i^1(x_i) \cdots g_i^{m_i}(x_i)]$ where $g_i^j(x_i) \in \mathbb{R}^{n_i}$, $j = 1 \cdots m_i$ and $W_{i,j}(x_i) = [w_{i,j}^1(x_i) \cdots w_{i,j}^{n_j}(x_i)]$ where $w_{i,j}^k(x_i) \in \mathbb{R}^{n_i}$, $k = 1 \cdots n_j$ constitute the process model for the i^{th} unit. $W_{i,j}$ captures the effect of the j^{th} unit on the i^{th} unit. It is assumed that the origin, $x_i = \mathbf{0}$, $i = 1 \cdots M$ is the nominal

equilibrium point for each unit. Functions $f_i(x_i)$, $G_i(x_i)$ and $W_{i,i-1}(x_i)$, $i = 1 \cdots M$ are assumed to be sufficiently smooth on their domain of definition. The units are connected in series via material or energy streams. The results in the chapter are applicable to system of the form of Eq.4.1, where evolution of the states in the i^{th} unit depends only on local states, local inputs and state variables of the preceding unit (through the interconnection $W_{i,i-1}(x_i)$ term). $V(x)$ is a Lyapunov function and $L_G V = [L_{g^1} V \ \cdots \ L_{g^m} V]$, $L_W V = [L_{w^1} V \ \cdots \ L_{w^p} V]$. The notation $B \backslash A$, where A and B are sets, refers to the relative complement, defined by $B \backslash A = \{x \in B : x \notin A\}$. Throughout the chapter, we assume that for any $u_i \in \mathbf{U_i}$ the solution of the each subsystem of Eq.4.1 exists and is continuous for all t, and we focus on the state feedback problem where $x_i(t)$, $i = 1 \cdots M$ is assumed to be available for all t.

4.2.2 Lyapunov-based predictive controller

In this section, we briefly review Lyapunov-based predictive controller designs (presented in Section 3.3.1) that handle non-linearity, uncertainty, input constraints and provide explicit characterization of stability region. We consider the k^{th} unit of the system in Eq.4.1 in fault-free scenario, i.e. $h_k(t) = 0$, (and drop the subscript k for simplicity) described by:

$$\dot{x} = f(x) + G(x)u + W(x)\theta \tag{4.2}$$

where x denotes process states of the process unit under consideration, u denotes the manipulated variables and θ is the vector of vanishing disturbances (in the sense that the nominal equilibrium point continues to be an equilibrium point in presence of disturbances; in context of multi-unit processes, θ denotes process state of upstream

unit).

Disturbance handling becomes all the more important in the context of multi-unit processes and we next review a robust predictive controller formulation that we will use to present the safe-parking framework. Specifically, in Chapter 3, a Lyapunov-based robust predictive controller is proposed that provides an explicit characterization of the stability region without using a min-max formulation and without assuming initial feasibility of the optimization problem. In the predictive control formulation of Chapter 3, the control action is computed by solving an optimization problem of Eqs. 3.8-3.12.:

To characterize the stability region for the Lyapunov-based robust MPC, a set Π is defined in Eq. 3.7 such that for all values of the state in the set Π, therefore, there exists a value of the manipulated variables 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.

$$\Omega := \{x \in \mathbb{R}^n : V(x) \leq c^{max}\} \tag{4.3}$$

where $c^{max} > 0$ is the largest number for which $\Omega \subseteq \Pi$. Stability and feasibility properties of the closed–loop system under the Lyapunov–based robust predictive controller are formalized in Theorem 3.1.

4.2.3 Safe-parking of an isolated unit

In this section, we briefly review the safe-parking framework for an isolated unit proposed in Chapter 2. To explain the safe-parking framework for an isolated unit, we again consider the k^{th} unit (Eq.4.2) in the plant presented in Section 4.2.1. Assume that a fault occurs in the first actuator $u^1(t)$ of the unit at time T^{fault} and reverts to fail-safe position u^1_{failed} with $u^1_{min} \leq u^1_{failed} \leq u^1_{max}$, and subsequently the fault is rectified at a time T^{repair}. This implies that $t^1_f = T^{fault}$ and $t^1_r = T^{repair}$. This leaves only u^i, $i = 2 \ldots m$ available during $T^{fault} < t \leq T^{repair}$ for feedback control of the unit. Examples of fail-safe positions include fully open for a valve controlling a coolant flow rate and fully closed for a valve controlling a steam flow etc. In this failure scenario, there exists a set of equilibrium points where the unit can be stabilized, which we denote as the candidate safe-park set:

$$X_c := \{x_c \in \mathbb{R}^n : f(x_c) + g^1(x_c)u^1_{failed} + \sum_{i=2}^{m} g^i(x_c)u^i = 0,\ u^i_{min} \leq u^i \leq u^i_{max},$$
$$i = 2, \ldots, m\} \tag{4.4}$$

The safe-park candidates therefore represent equilibrium points that the unit can be stabilized at, subject to the failed actuator, and with the other manipulated variables within the allowable ranges. Note that if $u^1_{failed} \neq 0$, then it may happen that $0 \notin X_c$, i.e., if the failed actuator is frozen at a non-nominal value, then it is possible that the unit simply cannot be stabilized at the nominal equilibrium point using the functioning control actuators. In other words, if one of the actuators fails and reverts to a fail-safe position, it may happen that no admissible combination of the functioning manipulated variables exists for which the nominal equilibrium point

continues to be an equilibrium point. If the controller attempts to use the functioning actuators to preserve nominal operation, it will not succeed since there does not exist an allowable value of the functioning inputs for which the nominal equilibrium point is still an equilibrium point. The states, in such an event, could possibly stabilize at an equilibrium point outside the stability region of the nominal equilibrium, thus making it impossible to resume nominal operation upon fault rectification. Even if it may be possible to resume nominal operation, it might not be the optimal way of resuming nominal operation. Thus choice of the temporary operating point is crucial for safety and performance of process operation. In Chapter 2, the safe-parking problem is defined as the one of identifying safe-park points $x_s \in X_c$ that allow efficient resumption of nominal operation upon fault-repair.

The key requirements for the choice of safe-park point are:

1. It should be possible to drive the process to the safe-park point from the nominal equilibrium point.

2. The safe-park point should be an equilibrium point corresponding to allowable values of manipulated variables in faulty scenario, and

3. It should be possible to resume nominal operation after the fault is rectified.

In Chapter 2, to account for constraints on inputs and nonlinearity, a safe-parking framework is developed that imposes the following criteria on the safe-park point: 1) the unit state at the time of failure resides in the stability region of the safe-park candidate (subject to depleted control action), so the process can be driven to the candidate safe-park point and 2) the safe-park candidate resides within the stability region of the nominal control configuration so the unit can be returned to nominal operation after

fault repair. These requirements are formalized in Theorem 4.1 below. To this end, consider the unit of Eq.4.2 for which the first control actuator fails at a time T^{fault} and is reactivated at time T^{repair}, and for which the stability region under nominal operation, denoted by Ω_n, has been characterized for the robust model predictive controller of Eqs.3.8–3.12. Similarly, for a candidate safe-park point x_c, we denote Ω_c as the stability region (computed a priori) and $u_n = u_{MPC}(x, x_n, u_{min}^{x_n}, u_{max}^{x_n}, \theta_{min}, \theta_{max})$ and $u_{x_c} = u_{MPC}(x, x_c, u_{min}^{x_c}, u_{max}^{x_c}, \theta_{min}, \theta_{max})$, where $u_{min}^{x_n}$, $u_{max}^{x_n}$ and $u_{min}^{x_c}$, $u_{max}^{x_c}$ denote the constraints on the manipulated variables for stabilizing the process at the nominal and safe-parking point respectively. As these controllers are designed to stabilize the process at two different operating points, the values of nominal manipulated variables for both controllers are different. This in turn leads to different values of u_{min} and u_{max} in the controller design.

Theorem 4.1. [Chapter 2] *Consider the constrained system of Eq.4.2 under the robust model predictive controller of Eqs.3.8–3.12 designed to achieve (using Theorem 3.1)* $\limsup_{t\to\infty} \|x(t)\| \leq \epsilon$ *where* ϵ *is a given positive real number. If* $x(0) \in \Omega_n$, $x(T^{fault}) \in \Omega_c$ *and* $\Omega_c \subset \Omega_n$, *then the switching rule*

$$u(t) = \left\{ \begin{array}{lll} u_n & , & 0 \leq t < T^{fault} \\ u_{x_c} & , & T^{fault} \leq t < T^{repair} \\ u_n & , & T^{repair} \leq t \end{array} \right\} \tag{4.5}$$

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

In Theorem 4.1, $x(T^{fault}) \in \Omega_c$ ensures that the process can be driven to the safe-park point in failure scenario thus satisfy the first requirement for safe-parking.

Also, as $\Omega_c \subset \Omega_n$, we have that $x(t) \in \Omega_n \; \forall \; T^{fault} \leq t < T^{repair}$. This means upon fault recovery the process can be driven back to the nominal operating point. This fulfills the third requirement for safe-parking. As the safe-park point is chosen from the set X_c, it is an equilibrium point in the faulty scenario thus satisfying the second requirement for safe-parking. The theorem guarantees that the process can be driven to the desired neighborhood of the origin (characterized by ϵ which can be made as small as desired) where the robust predictive controller of Theorem 3.1 is designed to drive it to.

Theorem 4.1 addresses the problem of safe-parking of an isolated unit, and considers neither the effect of safe-parking a unit on downstream plant operation, nor the effect of changes in upstream operation on the ability to safe-park a unit in question. Note that in a plant-wide setting, a change in operation of a unit naturally enters as a 'disturbance' in the downstream unit. Preparatory to the presentation of our results on a safe-parking framework for plant-wide fault-tolerant control, we characterize the maximum disturbance caused by safe-parking of unit k in Proposition 4.1 below.

Proposition 4.1. Consider operation of the k^{th} unit under the safe-parking framework of Theorem 4.1. If $x(0) \in \Omega_n$, then $\exists \; \alpha^i, \; i = 1 \cdots n_k$ such that $||x^i(t)|| \leq \alpha^i, \; i = 1 \cdots n_k, \; \forall t \geq 0$

Proof of Proposition 4.1: The proof of the proposition follows from Theorem 4.1. Since Ω_n is characterized by the level sets of the Lyapunov function, $\exists \; \alpha^i$ such that $x \in \Omega_n \implies ||x^i|| \leq \alpha^i, \; i = 1 \cdots n_k$. The fact that $x(t) \in \Omega_n \; \forall \; t \geq 0$ results in $||x^i(t)|| \leq \alpha^i, \; i = 1 \cdots n_k, \; \forall t \geq 0$. ■

4.3 Safe-parking framework for plant-wide fault-tolerant control

In Section 4.2.3, we reviewed the safe-parking procedure for an isolated unit. Almost always, a chemical plant consists of many process units which are connected via material, energy, and/or communication streams. A change in operating condition of one unit, therefore, enters the downstream unit as a disturbance and, hence, huge change in operating condition of one unit can jeopardize plant operation. Specifically, consider a multi-unit plant in which due to failure in one unit, the unit is safe-parked using the framework presented in Section 4.2.3, without considering its interaction with the other units in the plant. In such a case, it may happen that even though the faulty unit is safely operated at safe-park point, the change in operation of the faulty unit may cause a significantly large disturbance to downstream units (i.e. the disturbance can not be rejected in the downstream units) or may even result in instability. This necessitates that the safe-park point for the faulty unit be chosen with proper consideration to its effect on downstream processes. In other words, a safe-park point should be chosen such that it has minimal adverse effect on the ability of downstream unit to continue nominal operation. In this section, we present a framework to account for the interaction of faulty units with downstream operation while choosing a safe-park point for the faulty unit.

4.3.1 Problem definition

We consider the scenario where one of the control actuators in unit k ($k \in [1\, M]$) fails and reverts to the fail-safe value. Specifically, we consider a fault occurring,

without loss of generality, in the first control actuator of the k^{th} unit at a time T^{fault}, subsequently rectified at a time T^{repair} i.e. $t^1_{k,f} = T^{fault}$ and $t^1_{k,r} = T^{repair}$. The process model for the faulty unit (k^{th} unit) in failure scenario can be given as,

$$\dot{x}_k = f_k(x_k) + g^1_k(x_k)u^1_{k,failed} + \sum_{j=2}^{m_k} g^j_k(x_k)u^j_k + W_{k,k-1}(x_k)x_{k-1} \tag{4.6}$$

This leaves only u^j_k, $j = 2 \ldots m_k$ available for feedback control of the k^{th} unit. As explained in Section 4.2.3, if $u^1_{k,failed} \neq 0$, then the origin (the nominal operating point of k^{th} unit) may no longer be an equilibrium point and hence, the k^{th} unit can no longer be operated at the nominal equilibrium point necessitating safe-parking of the k^{th} unit.

The change in operating condition of the faulty unit (k^{th} unit) due to safe-parking, however, enters the downstream unit as a disturbance. If this disturbance is 'small enough' (as defined in Section 4.3.2), then it can be rejected in the $k+1^{th}$ unit (i.e., in spite of change in inlet condition of $k+1^{th}$ unit, the $k+1^{th}$ unit can be maintained at nominal operation by changing the nominal values of the manipulated variables), and the rest of the plant can, therefore, be operated nominally. Another possibility is that, if the disturbance caused by safe-parking of k^{th} unit is very large and it may not be rejected in the $k+1^{th}$ unit, then the downstream $k+1^{th}$ unit cannot continue operation at the nominal operating point. In other words, operation of the faulty unit at the safe-park point does not allow nominal operation of the downstream unit. This then necessitates safe-parking of the $k+1^{th}$ unit to avoid any undesirable incident requiring the simultaneous safe-parking of two units.

We first consider the case where the safe-parking produces 'small disturbance' to the downstream unit. We formalize, in Section 4.3.2, the framework to define 'small

disturbance' and thus to choose safe-park point so that the downstream unit can continue nominal operation. Next in Section 4.3.3, we consider the case where no safe-park point for the faulty unit exists which allows nominal operation of downstream operation and we present the framework for simultaneous safe-parking of multiple units. Efficacy of the proposed framework is demonstrated by simulation study on a two-unit chemical process in Section 4.4.

4.3.2 Safe-parking of a single unit in a multi-unit process

Consider the fault scenario described in Section 4.3.1 where an actuator of the k^{th} unit fails such that nominal operation in the unit cannot be continued and so safe-parking of the k^{th} unit is inevitable to continue safe operation of the whole plant. As discussed earlier, the choice of a safe-park point for the k^{th} unit allows the safe-operation in the k^{th} unit during fault rectification and ensures resumption of nominal operation in the k^{th} unit upon fault repair. In the multi-unit setup, an additional criterion needs to be added to the choice of safe-park point which is that if possible, it should allow continued nominal operation in the downstream units. In this section, we provide a systematic procedure to choose safe-park point that allows continued nominal operation in the downstream units. Preparatory to the presentation of the results, we define the set:

$$\begin{aligned} D_k = &\{x_k \in \mathbb{R}^{n_k} : f_{k+1}(x_{k+1,ss}) + G_{k+1}(x_{k+1,ss})u_{k+1} + W_{k+1,k}(x_{k+1,ss})x_k = 0, \\ &u_{k+1} \in U_{k+1} \in \mathbb{R}^{m_{k+1}}\} \end{aligned} \tag{4.7}$$

where $x_{k+1,ss}$ is the nominal operating points in the $k+1^{th}$ unit. Therefore, D_k is the set of values of process variables (x_k) in the k^{th} unit such that if the k^{th} unit is stabilized at x_k, nominal operation in the $k+1^{th}$ unit can be maintained using allowable, although possibly different from nominal, values of the manipulated variables in the $k+1^{th}$ unit. In other words, the non-vanishing disturbance caused by change in operation of the k^{th} unit can be rejected in the $k+1^{th}$ unit at steady state via using non-nominal values of the manipulated variables. Note that $h_{k+1} = 0$ is used for calculation of the set D_k because there is no fault in the $k+1^{th}$ unit. We denote $u_{k+1,n} = u_{MPC}(x_{k+1}, x_{k+1,n}, u^{x_n}_{k+1,min}, u^{x_n}_{k+1,max}, \theta_{k+1,min}, \theta_{k+1,max})$ as the controller designed to control the $k+1^{th}$ unit at the nominal operating point with nominal values of manipulated variables. As mentioned earlier, when the k^{th} unit is safe-parked, the controller in $k+1^{th}$ unit can maintain the nominal operation in the unit using non-nominal values of the manipulated variables. We denote this controller as $u'_{k+1,n} = u_{MPC}(x_{k+1}, x_{k+1,n}, u'_{k+1,min}, u'_{k+1,max}, \theta_{k+1,min}, \theta_{k+1,max})$ where $u'_{k+1,min}$ and $u'_{k+1,max}$ are modified constraints on manipulated variables. Both $u_{k+1,n}$ and $u'_{k+1,n}$ are designed to stabilize the $k+1^{th}$ unit at the nominal equilibrium point but as the nominal values of the manipulated variables (and therefore of the constraints) are different for these controllers, they may have different stability regions which we denote by $\Omega_{k+1,n}$ and $\Omega'_{k+1,n}$ respectively. As before, we denote $\Omega_{k,n}$ and $\Omega_{k,c}$ as the stability region for nominal equilibrium point and the safe-park point for the k^{th} unit respectively. For a choice of safe-park point of the k^{th} unit, the maximum disturbance caused to the $k+1^{th}$ unit is denoted by $d_{k,max}$ (characterized using Proposition 4.1). Theorem 4.2 below provides the key requirements for choice of the safe-park point for the faulty unit so that the downstream units can continue nominal operation.

Theorem 4.2. *Consider the constrained system of Eq.4.1 subject to failure in the first control actuator of the k^{th} unit at a time T^{fault}, subsequently rectified at a time T^{repair}. If $x_k(0) \in \Omega_{k,n}$ and $x_{k+1}(0) \in \Omega_{k+1,n}$, $x_{k,sf}$ is the safe-park point for the k^{th} unit satisfying $x_k(T^{fault}) \in \Omega_{k,c}$, $x_{k,sf} \in D_k$ and $\Omega_{k,c} \subset \Omega_{k,n}$ and if $x_{k+1}(T^{fault}) \in \Omega'_{k+1,n}$ then the switching rule*

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

under the robust model predictive controller of Eqs.3.8-3.12 with $\theta_{k+1,min} = -d_{k,max}$ and $\theta_{k+1,max} = d_{k,max}$, guarantees that $x_k(t) \in \Omega_{k,n}$, $x_{k+1}(t) \in \Omega_{k+1,n}$ for $\forall t \geq 0$ and $\limsup_{t\to\infty} \|x_k(t)\| \leq \epsilon_k$ and $\limsup_{t\to\infty} \|x_{k+1}(t)\| \leq \epsilon_{k+1}$ where ϵ_k and ϵ_{k+1} are given positive real numbers.

Proof of Theorem 4.2: Since $x_k(T^{fault}) \in \Omega_c$ and $\Omega_c \subset \Omega_n$ the switching rule of Theorem 4.1 guarantees that $x_k(t) \in \Omega_{k,n}$ $\forall\, t \geq 0$ and $\limsup_{t\to\infty} \|x_k(t)\| \leq \epsilon_k$. By invoking Proposition 4.1, we know that $|x^i_k(t)| \leq d^i_{k,max}$, $i = 1 \cdots n_k$, $\forall t \geq 0$. Therefore, designing the robust predictive controller for the $k+1^{th}$ unit with $\theta_{k+1,min} = -d_{k,max}$, $\theta_{k+1,max} = d_{k,max}$ and with $x_{k+1}(0) \in \Omega_{k+1,n}$, satisfies all the requirements of Theorem 3.1. Therefore, for all $0 \leq t \leq T^{fault}$, $x_{k+1}(t) \in \Omega_{k+1,n}$. Since $x_{k+1}(T^{fault}) \in \Omega'_{k+1,n}$, it follows that $x_{k+1}(t) \in \Omega'_{k+1,n}$ $\forall$ $T^{fault} \leq t \leq T^{repair}$. Since $\Omega_{k+1,n}$ and $\Omega'_{k+1,n}$ are defined by different values of the level sets for the same Lyapunov function (and the controllers $u_{k+1,n}$ and $u'_{k+1,n}$ enforce a decay of the same Lyapunov function), and $x_{k+1}(0) \in \Omega_{k+1,n}$, it follows that $x_{k+1}(T^{fault}) \in \Omega_{k+1,n}$ and $x_{k+1}(t) \in \Omega_{k+1,n}$ $\forall$ $T^{fault} \leq$

$t \leq T^{repair}$. This leads to $x_{k+1}(T^{repair}) \in \Omega_{k+1,n}$. $x_{k+1}(t) \in \Omega_{k+1,n}$ for $\forall t \geq 0$ and $\limsup_{t\to\infty} \|x_{k+1}(t)\| \leq \epsilon_{k+1}$ therefore follow. This completes the proof of Theorem 4.2. ■

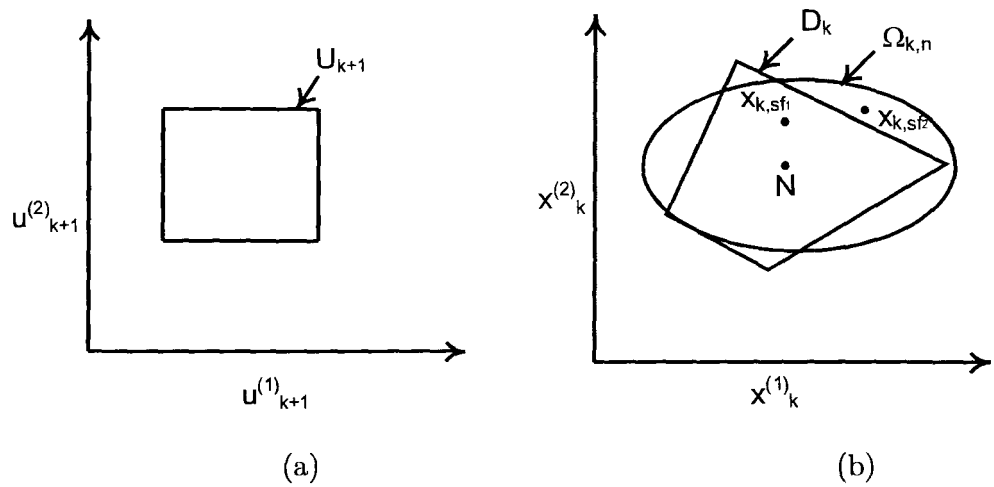


Figure 4.1: Graphical illustration of requirements of Theorem 4.2 showing (a) constraints on inputs of downstream unit ($k+1^{th}$ unit), and (b) the corresponding set D_k and stability region ($\Omega_{k,n}$)of nominal equilibrium point of faulty unit (k^{th} unit). The set D_k represents the allowable values of equilibrium points for the k^{th} unit, such that with allowable values of the inputs in the $k+1^{th}$ unit, the nominal equilibrium point continues to be an equilibrium point for the $k+1^{th}$ unit.

Remark 4.1. The key idea in Theorem 4.2 is to ensure that there exist admissible values of the manipulated variables in the downstream unit which can 'reject' the effect of safe-parking the faulty unit to preserve nominal operation of the downstream unit. This requirement is graphically illustrated in Fig.4.1. Fig.4.1a depicts constraints on the inputs of the $k+1^{th}$ unit. These constraints correspond to values of the process states of the k^{th} unit shown by the set D_k in Fig.4.1b such that for any value of the process states of the k^{th} unit in the set D_k, the nominal values of

the manipulated inputs in the $k+1^{th}$ unit can be adjusted to preserve nominal operation in the $k+1^{th}$ unit. Superimposed is also the stability region of the nominal equilibrium point ($\Omega_{k,n}$) for the k^{th} unit and two candidate safe-park points x_{k,sf_1} and x_{k,sf_2}. Note that the candidate safe-park point x_{k,sf_2} would be an acceptable safe-park point in an isolated unit (since $x_{k,sf_2} \in \Omega_{k,n}$ guaranteeing the resumption of nominal operation in the k^{th} unit after the fault rectification). It is, however, not an acceptable safe-park point from the viewpoint of preserving nominal operation in the downstream unit since $x_{k,sf_2} \notin D_k$. In contrast, the candidate safe-park point x_{k,sf_1} guarantees the resumption of nominal operation in the k^{th} unit as well as the continuation of nominal operation in the $k+1^{th}$ unit during the fault rectification since $x_{k,sf_1} \in \Omega_{k,n} \cap D_k$ and therefore x_{k,sf_1} is an acceptable choice for safe-parking of the k^{th} unit in a plant setting.

Remark 4.2. Note that the $k+1^{th}$ unit is operated (and controlled) using a controller that uses a non-nominal value of the manipulated input, and therefore has a different stability region (denoted by $\Omega'_{k+1,n}$). The stability region, however, is still described by the same Lyapunov function (and the same Lyapunov function is used in the control design as well). Since the state for the $k+1^{th}$ unit is initially inside the stability region under nominal operation of the $k+1^{th}$ unit and the controller for the $k+1^{th}$ unit ensures continued decay of the Lyapunov function, $x_{k+1}(T^{fault}) \in \Omega_{k+1,n}$ follows. Theorem 4.2 requires that $x_{k+1}(T^{fault}) \in \Omega'_{k+1,n}$. This leads to two possibilities: $\Omega'_{k+1,n} \supset \Omega_{k+1,n}$ and $\Omega'_{k+1,n} \subset \Omega_{k+1,n}$. In either case, since the controller during T^{fault} and T^{repair} enforces decay of the same Lyapunov function describing $\Omega_{k+1,n}$ and $\Omega'_{k+1,n}$, $x_{k+1}(T^{repair}) \in \Omega_{k+1,n}$ follows, i.e., the state residing in the stability region at the time of fault repair is guaranteed and not required in Theorem 4.2.

Remark 4.3. Note that the set D_k is based on steady-state considerations and its characterization is computationally inexpensive. Specifically, it involves only repeated solving of the algebraic equation:

$$f_{k+1}(x_{k+1,ss}) + G_{k+1}(x_{k+1,ss})u_{k+1} + W_{k+1,k}(x_{k+1,ss})x_{k,sf} = 0 \tag{4.8}$$

Furthermore, the equation is linear in the variables of interest (x_k, u_k). For fixed (and known) values of $x_{k+1,ss}$, the equation takes the form:

$$A + Bu_{k+1} + Cx_{k,sf} = 0 \tag{4.9}$$

where $A \in \mathbb{R}^{n_{k+1} \times 1}$, $B \in \mathbb{R}^{n_{k+1} \times m_{k+1}}$ and $C \in \mathbb{R}^{n_{k+1} \times n_k}$ are constant matrices. The set D_k can readily be computed by varying u_{k+1} over the desired values and computing the corresponding values of $x_{k,sf}$. Note that while the schematic in Fig.4.1 shows the two dimensional representation to illustrate the key idea, this visual representation is not necessary for the purpose of implementation of the proposed safe-parking framework. In particular, verification of the presence of a point in the set D_k can be done via solving a linear equation of the form of Eq.4.9, and the presence in the set $\Omega_{k,n}$ can be verified via evaluating the Lyapunov function (again an algebraic evaluation). Also, note that the characterization of the set X_c, stability region for nominal equilibrium point & safe-park points and computation of the set D_k can be done off-line.

Remark 4.4. Note that there may be instances when the requirements of Theorem 4.2 are not satisfied, i.e., there simply does not exist a safe-parking point that enables nominal operation of the downstream units. Such possibilities are handled in

Section 4.3.3. However, the value of Theorem 4.2 is in that it explores the possibility of continued operation of the plant (if possible) in a way that preserves nominal operation. In other words, even in the presence of a fault in a mid-stream unit, the faulty unit is safe-parked to prevent onset of hazardous situations, enable smooth resumption of nominal operation in the faulty unit, as well as enabling the subsequent unit to continue nominal operation, thereby not disrupting the production of valuable products.

4.3.3 Simultaneous safe-parking of multiple units

In the last section, we presented the framework to select a safe-park point so that nominal operation in downstream units can be continued. However, it may happen that in case of a fault, none of the candidate safe-park points satisfy the requirements presented in Theorem 4.2, i.e. $\Omega_{k,n} \cap D_k \cap X_{k,c} = 0$. In other words, there exist no safe-park point such that nominal operation of the downstream unit can be continued. This necessitates that the downstream unit also be safe-parked. However, due to the interconnected nature of the process, the procedure for safe-parking of isolated units cannot be duplicated to safe-park multiple units, and one needs a framework to simultaneously safe-park multiple units to continue the safe-operation of the entire plant. In this section, we provide details of the framework to carry out simultaneous safe-parking.

Consider the plant of Eq.4.1 with $\Omega_{k,n} \cap D_k \cap X_{k,c} = 0$. Preparatory to presenting the framework for simultaneous safe-parking, we recall the control laws $u_{k,n}$, u_{k,x_c} and $u_{k+1,n}$ as defined in Section 4.3.2. Further, we define,

$u_{k+1,x_c} = u_{MPC}(x_{k+1}, x_{k+1,c}, u_{k+1,min}^{x_{k+1,c}}, u_{k+1,max}^{x_{k+1,x_c}}, \theta_{k+1,min}, \theta_{k+1,max})$ as control law to

stabilize the $k+1^{th}$ unit at a candidate safe-park point $x_{k,c}$. Also, we define $\Omega_{k+1,n}$ and $\Omega_{k+1,c}$ as the stability regions for the nominal equilibrium point and safe-park point in the downstream unit, for the robust predictive controller of Eqs.3.8–3.11 designed using $\theta_{k+1,min} = -d_{k,max}$ and $\theta_{k+1,max} = d_{k,max}$ where $d_{k,min}$ and $d_{k,max}$ are maximum possible disturbance that can be caused by safe-parking of k^{th} unit (characterized using Proposition 4.1). The key idea in simultaneous safe-parking is to ensure that for a choice of safe-park point of the faulty processing unit, there exists a safe-park point for the downstream unit (for which the 'disturbance' caused by the safe-parking of the faulty unit can be rejected) and such that it can resume nominal operation when the faulty processing unit reverts to nominal operation. This requirement is formalized in Theorem 4.3 below.

Theorem 4.3. *Consider the constrained system of Eq.4.1 subject to failure in the first control actuator of the k^{th} unit at a time T^{fault}, subsequently rectified at a time T^{repair}, and $x_{k,sf}$ and $x_{k+1,sf}$ are chosen as safe-park points for the k^{th} and $k+1^{th}$ unit, respectively, such that $x_k(T^{fault}) \in \Omega_{k,c}$, $x_{k+1}(T^{fault}) \in \Omega_{k+1,c}$, $\Omega_{k,c} \subset \Omega_{k,n}$ and $\Omega_{k+1,c} \subset \Omega_{k+1,n}$, then the switching rule*

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

under the robust model predictive controller of Eqs.3.8-3.12, guarantees that $x_k(t) \in \Omega_{k,n}$ and $x_{k+1}(t) \in \Omega_{k+1,n}$ for $\forall t \geq 0$, $\limsup_{t\to\infty} \|x_k(t)\| \leq \epsilon_k$ and $\limsup_{t\to\infty} \|x_{k+1}(t)\| \leq \epsilon_{k+1}$.

Proof of Theorem 4.3:

For the k^{th} unit, since $x_k(T^{fault}) \in \Omega_{k,c}$ and $\Omega_{k,c} \subset \Omega_{k,n}$, from Theorem 4.1, $x_k(t) \in \Omega_{k,n}$ for $\forall t \geq 0$ and $\limsup_{t\to\infty} \|x_k(t)\| \leq \epsilon_k$ follows.

The robust model predictive controller for the $k+1^{th}$ unit is designed with $\theta_{k+1,min} = -d_{k,max}$ and $\theta_{k+1,max} = d_{k,max}$. Also, $x_{k+1}(T^{fault}) \in \Omega_{k+1,c}$ and $\Omega_{k+1,c} \subset \Omega_{k+1,n}$, it follows from Theorem 3.1 that $x_{k+1}(t) \in \Omega_{k+1,n}$ for $\forall t \geq 0$ and $\limsup_{t\to\infty} \|x_{k+1}(t)\| \leq \epsilon_{k+1}$.■

Remark 4.5. Note that unlike Theorem 4.2, the unit downstream to the faulty unit does not require to preserve nominal operation. In designing the controller for the safe-parking of the downstream unit as well as for nominally operating the downstream unit, the fact that an upstream faulty unit could safe-park has to be accounted for, and this is achieved in Theorem 4.3 by designing the controllers for the downstream unit such that it can reject the disturbance caused by the faulty unit. In picking the safe-park point for $k+1^{th}$ unit, one can additionally incorporate further considerations to ensure that the units further downstream can preserve nominal operation. This can be done by requiring that the safe-park point for the $k+1^{th}$ unit be such that it also satisfies $x_{k+1,sf} \in D_{k+1}$. This allows nominal operation in units downstream to the $k+1^{th}$ unit even though both k^{th} and $k+1^{th}$ unit are safe-parked. If it so happens that there exists no safe-park point for unit k to unit $k+p-1$ such that nominal operation in downstream units can be continued, then a combination of the procedures of Theorem 4.2 and Theorem 4.3 can be utilized to simultaneously safe-park unit k to unit $k+p$ to preserve nominal operation (if possible) of the rest of the plant.

Remark 4.6. The proposed framework considers plants where units are connected in series. The framework, however can be readily extended to plants where units

are connected in a combination of parallel and series fashions. To this end, the safe-park point for faulty unit would have to be chosen using stability region for the unit and the D_k estimated for each of downstream units that are directly connected to the faulty k^{th} unit. The safe-park point would have to be chosen such that $x_{k,sf}$ resides in $\Omega_{k,n}$ and all D_k. Furthermore, the robust predictive controller for each downstream unit would have to be designed to reject maximum disturbance caused by any of the upstream unit. To deal with recycle, on the other hand, the process will have to be divided into sub-processes (not necessarily the same as individual units) that would eventually result in the hierarchical structure of Eq.4.1). A detailed analysis of processes with recycle, however, remains outside the scope of the present work.

Remark 4.7. Note that while the safe-parking framework is presented assuming fault in one of the actuators in the unit, it can be readily extended to multiple faults occurring simultaneously. When there are multiple faults occurring in the unit, the candidate safe-park points and corresponding stability regions should be calculated using failed value for all failed actuators and then a safe-park point should be chosen using safe-parking framework to ensure safe operation of the entire plant. Thus, generalization to multiple faults (simultaneous or otherwise), while increasing off-line computational cost (due to the necessity of determining the safe-park points for all possible combinations of the faults in the control actuators), is possible in the proposed framework.

Remark 4.8. Note that while the safe-parking Theorems 4.2 and 4.3 utilize 'worst-case' estimates of the effect of safe-parking a unit to compute the relevant stability region estimates, the current (as well as estimated future trajectories) of the disturbances can be made available to the downstream controllers resulting in a significantly

improved performance. Specifically, when deriving guarantees for safe-parking the units it is necessary to use the worst case effect of safe-parking a unit since the exact profile of the state variables depends on the process state when the fault takes place. However, once a fault takes place, the current value of the process states of the faulty unit (which act as 'disturbance' to the downstream unit) can be used in computing and improving the control action in the downstream unit (for a demonstration of the improved performance using this idea, see the simulation example).

Remark 4.9. While the results in the present chapter are derived assuming availability of full state feedback, the framework can be extended to handle availability of limited measurements. However, to do this, the stability regions for the various operating points in the multi-unit setting would have to be modified to the corresponding output-feedback stability region, and the controllers would have to be augmented with appropriate state observers (similar to the generalization of safe-parking of an isolated unit presented in Chapter 3 to handle availability of limited measurements). Note also that the use of predictive controllers allows explicit handling of time-delays between subsequent units. Application of the proposed framework under limited measurements and time delays, however, remains outside the scope of the present work.

4.4 Application to a two-unit chemical process

To demonstrate the efficacy of the proposed safe-parking framework for multi-unit processes, we perform simulation study on a plant comprising of two chemical reactors in series (also used in El-Farra et al. [2005] in the context of fault-tolerant control using communication networks). To this end, consider a process composed of

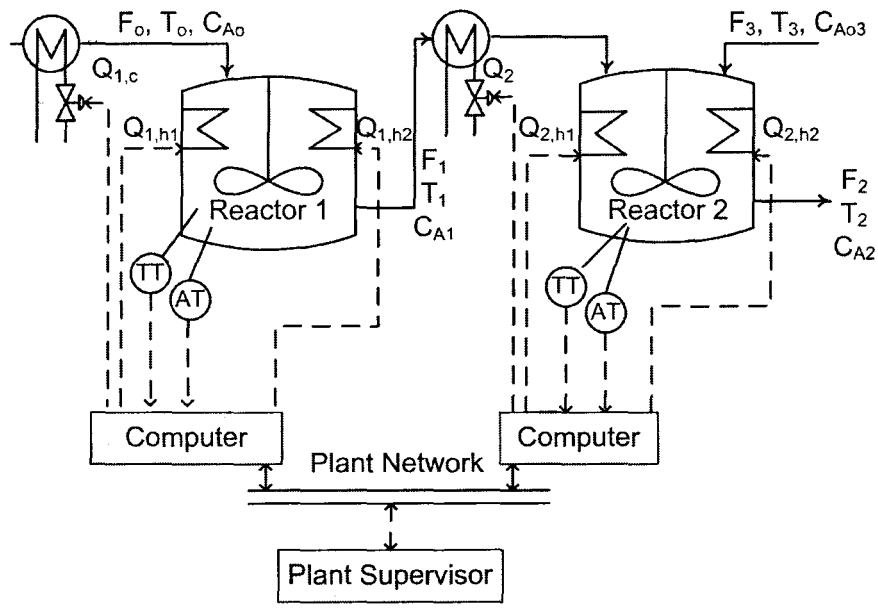


Figure 4.2: Schematic of the process with two chemical reactors.

two well-mixed, non-isothermal continuous stirred-tank reactors (CSTRs) with interconnections, where three parallel irreversible elementary exothermic reactions of the form $A \xrightarrow{k_1} B$, $A \xrightarrow{k_2} U$ and $A \xrightarrow{k_3} R$ take place, where A is the reactant species, B the desired product, and U and R are the undesired byproducts. As shown in Fig.4.2, the feed to CSTR-1 consists of pure A at flow rate F_0, molar concentration C_{A0}, and temperature T_0, and the feed to CSTR-2 consists of the output of CSTR-1, and an additional fresh stream feeding pure A at flow rate F_3, molar concentration C_{A03}, and temperature T_{03}. Due to the nonisothermal nature of the reactions, a heat-exchanger at the inlet of the reactors is used to remove heat and two coils are used to add heat in each reactor. Under standard modeling assumptions, a mathematical model of the

plant can be derived and takes the following form:

$$\frac{dT_1}{dt} = \frac{F_0}{V_1}(T_0 - T_1) + \sum_{i=1}^{3} \frac{\Delta H_i}{\rho c_p} R_i(C_{A1}, T_1) + \frac{Q_1}{\rho c_p V_1} \tag{4.10}$$

$$\frac{dC_{A1}}{dt} = \frac{F_0}{V_1}(C_{A0} - C_{A1}) - \sum_{i=1}^{3} R_i(C_{A1}, T_1) \tag{4.11}$$

$$\frac{dT_2}{dt} = \frac{F_1}{V_2}(T_1 - T_2) + \frac{F_3}{V_2}(T_{03} - T_2) + \sum_{i=1}^{3} \frac{\Delta H_i}{\rho c_p} R_i(C_{A2}, T_2) + \frac{Q_2}{\rho c_p V_2} \tag{4.12}$$

$$\frac{dC_{A2}}{dt} = \frac{F_1}{V_2}(C_{A1} - C_{A2}) + \frac{F_3}{V_2}(C_{A03} - C_{A2}) - \sum_{i=1}^{3} R_i(C_{A2}, T_2) \tag{4.13}$$

where $R_i(C_{Aj}, T_j) = k_{i0} exp(E_i/RT_j) C_{Aj}$, for $j = 1, 2$. The symbols T, C_A, Q, and V denote the temperature of the reactor, the concentration of species A, the rate of heat input/removal from the reactor, and the volume of reactor, respectively, with subscript 1 denoting CSTR 1, and subscript 2 denoting CSTR 2. ΔH_i, k_i, E_i, $i = 1, 2, 3$, denote the enthalpies, pre-exponential constants and activation energies of the three reactions, respectively, c_p and ρ denote the heat capacity and density of fluid in the reactor. Q_1 and Q_2 are net heat added/removed from CSTR-1 and CSTR-2, respectively. The Q_1 term consists of heat removed $Q_{1,c}$ and heat added $Q_{1,h1}$ and $Q_{1,h2}$ (i.e. $Q_1 = Q_{1,c} + Q_{1,h1} + Q_{1,h2}$) in CSTR-1 while Q_2 consists of heat removed $Q_{2,c}$ and heat added $Q_{2,h1}$ and $Q_{2,h2}$ (i.e. $Q_2 = Q_{2,c} + Q_{2,h1} + Q_{2,h2}$) in CSTR-2. The values for all the parameters is given in Table 4.1.

The control objective is to stabilize CSTR-1 at the unstable equilibrium point (C_{A1} = 1.69 kmol/m^3, T_1 = 424.4 K) and CSTR-2 at the unstable equilibrium point (C_{A2} = 0.89 kmol/m^3, T_2 = 444.5 K). The manipulated variables for the CSTR-1 are inlet concentration (C_{A0}) and heat removed/added (Q_1) while manipulated variables for the CSTR-2 are inlet concentration of stream 3 (C_{A30}) and heat

Table 4.1: Process Parameters and Steady-State Values for the Chemical Reactors of Eq.4.10

Parameter	Value	Unit	Parameter	Value	Unit
F_0	4.998	m^3/hr	E_3	7.53×10^4	kJ/kmol
F_1	4.998	m^3/hr	ρ	2000	Kg/m^3
F_3	8	m^3/hr	c_p	0.731	KJ/(kgK)
V_1	1	m^3	T_{1s}	424.4	K
V_2	3	m^3	C_{A1s}	1.69	$kmol/m^3$
R	8.314	KJ/(kmolK)	T_{2s}	444.5	K
T_0	280	K	C_{A2s}	0.89	$kmol/m^3$
T_{03}	280	K	$Q_{1,c,max}$	0	KJ/hr
C_{A0s}	2.4	$kmol/m^3$	$Q_{1,c,min}$	-2×10^6	KJ/hr
C_{A03s}	2.6	$kmol/m^3$	$Q_{1,h1,max}$	0.5×10^6	KJ/hr
Q_{1s}	0.7×10^6	KJ/hr	$Q_{1,h1,min}$	0	KJ/hr
Q_{2s}	0.3×10^6	KJ/hr	$Q_{1,h2,max}$	1.5×10^6	KJ/hr
ΔH_1	1.00×10^5	kJ/kmol	$Q_{1,h2,min}$	0	KJ/hr
ΔH_2	1.04×10^5	kJ/kmol	$Q_{2,c,max}$	0	KJ/hr
ΔH_3	1.08×10^5	kJ/kmol	$Q_{2,c,min}$	-2×10^6	KJ/hr
k_{10}	3.0×10^6	hr^{-1}	$Q_{2,h1,max}$	0.5×10^6	KJ/hr
k_{20}	3.0×10^5	hr^{-1}	$Q_{2,h1,min}$	0	KJ/hr
k_{30}	3.0×10^5	hr^{-1}	$Q_{2,h2,max}$	1.5×10^6	KJ/hr
E_1	5.0×10^4	kJ/kmol	$Q_{2,h2,min}$	0	KJ/hr
E_2	7.53×10^4	kJ/kmol			

removed/added (Q_2). Controller prescribed values of Q_1 and Q_2 are achieved by manipulating appropriate heating or cooling streams. The constraints on each input are given in Table 4.1. The constraints on net heat added/removed is $-2 \times 10^6 \leq Q_1 \leq 2 \times 10^6$ KJ/hr and $-2 \times 10^6 \leq Q_2 \leq 2 \times 10^6$ KJ/hr. The constraints on other inputs are $0 \leq C_{A0} \leq 8$ kmol/m^3 and $2.3 \leq C_{A3} \leq 2.9$ kmol/m^3. The nominal equilibrium points for CSTR-1 and CSTR-2 corresponds to manipulated variable values of $C_{A0} = 2.4$ kmol/m^3, $Q_1 = 0.7 \times 10^6$ KJ/hr and $C_{A3} = 2.6$ kmol/m^3, $Q_2 = 3 \times 10^5$ KJ/hr.

For stabilizing the process at the nominal equilibrium point, the robust Lyapunov-based model predictive controller of Section 4.2.2 is used for each CSTR. The robust Lyapunov-based MPC is designed using a quadratic Lyapunov function of the form $V_i = x_i^T P_i x_i;\ i = 1, 2$ with $P_1 = \begin{bmatrix} 2.37 & 0.09 \\ 0.09 & 0.02 \end{bmatrix}$ and $P_2 = \begin{bmatrix} 5.90 & 0.29 \\ 0.27 & 0.02 \end{bmatrix}$ (generated by solving Riccati equation of Eq. 2.2). The matrices in the objective function of Eq.3.12 are chosen as $Q_{w1} = Q_{w2} = \begin{bmatrix} 25 & 0 \\ 0 & \frac{1}{4} \end{bmatrix}$ and $R_{w1} = R_{w2} = \begin{bmatrix} \frac{5}{4} & 0 \\ 0 & \frac{5}{1 \times 10^6} \end{bmatrix}$ and an execution period of $\Delta_i = 0.01$ hr, $i = 1, 2$ is used for MPC implementation. The prediction and control horizons of 0.02 hr and 0.02 hr, respectively, are used in implementing the predictive controller in both units. It should be noted that as the stability of closed loop process system is guaranteed by use of stability constraint in the controller formulations, short prediction horizon are chosen to reduce on-line computational requirements. For implementation purpose, the robust predictive controller is discontinued once the process states reach the neighborhood of the desired equilibrium point and a stability constraint of the form $V_i(x_i(t + \Delta_i)) \leq 0.98 V_i(x_i(t))$ $i = 1, 2$ is incorporated in the optimization problem to guarantee stability of the closed–loop system.

We first demonstrate the implementation of Theorem 4.2 where it is possible to reject the disturbance caused by safe-parking of the faulty unit in the downstream unit (see Section 4.3.2). To this end, consider a fault where one of the heating coils in CSTR-1 fails to its fail-safe position (resulting in $Q_{1,h2} = 0$) at time $t = 1$ hr and so the constraints on net heat added/removed from CSTR-1 becomes $-2 \times 10^6 \leq Q_1 \leq 0.5 \times 10^6$ KJ/hr. This makes it impossible to operate CSTR-1 at the nominal equilibrium point because there exist no admissible inputs which can maintain CSTR-1 at the nominal equilibrium point and, therefore, CSTR-1 needs to be safe-parked at a safe-park point.

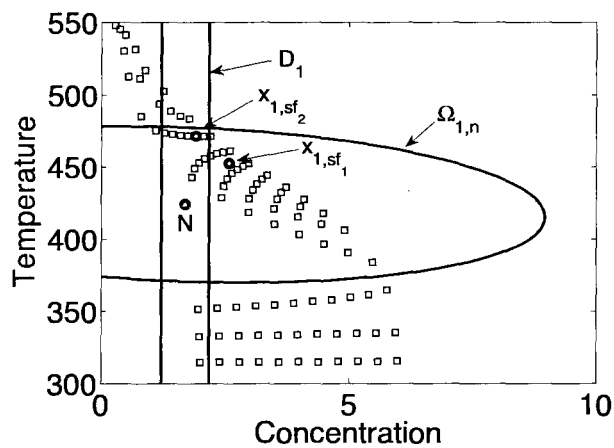


Figure 4.3: Stability region for nominal equilibrium point ($\Omega_{1,n}$), the set D_1 and candidate safe-park points (□) for fail-safe value of $Q_{1,h1}$ for CSTR-1. x_{1,sf_1} and x_{1,sf_2} are two representative candidate safe-park points where x_{1,sf_2} satisfies both the requirements of Theorem 4.2, allowing nominal operation in the downstream unit, while x_{1,sf_1} satisfies the requirements for the safe-parking of an isolated unit.

The stability region for CSTR-1 is estimated using grid search technique as described in Section 2.2.3 with grid interval of 1.67 °C and 0.04 Kmol/m^3. The stability

region is denoted by $\Omega_{1,n}$ in Fig.4.3. A discrete manifold of available candidate safe-park points is generated by solving the steady state system equations for allowable values of manipulated variables in the faulty scenario. A grid of manipulated variables with interval of 0.06 Kmol/m^3 and 0.1×10^6 KJ/s is used to generate the manifold and the manifold is shown in Fig.4.3 by $\square$.

To demonstrate the need for accounting for the multi-unit nature of the process, we first consider the case where a fault occurs in CSTR-1 and it is safe-parked utilizing the safe-parking framework for isolated unit described in Section 4.2.3. Therefore a safe-park point x_{1,sf_1} : (C_{A1} = 2.58 kmol/m^3, T_1 = 452.6 K) is chosen. Note that $x_{1,sf_1} \in \Omega_{k,n}$ and $N \in \Omega_{k,x_{1,sf_1}}$. It is therefore possible to stabilize CSTR-1 at the safe-park point x_{1,sf_1}. However, as can be seen from the dashed line in Fig.4.4, safe-parking CSTR-1 at x_{1,sf_1} does not permit operating CSTR-2 at the nominal equilibrium point. To explain this, we also compute the set D (defined in Eq.4.7) and superimpose on the candidate safe-park points in Fig.4.3. It can be seen that the safe-park point x_{1,sf_1} is outside the set D. This explains the inability of operating CSTR-2 at the nominal equilibrium point. In summary, as $x_{1,sf_1} \in \Omega$ the operation in CSTR-1 can be resumed after fault rectification but during fault rectification the final product quality cannot be maintained at desired specifications. In contrast, if the proposed safe-parking framework outlined in Theorem 4.2 is utilized, it dictates picking x_{1,sf_2} : (C_{A1} = 1.90 kmol/m^3, T_1 = 471.6 K) as the safe-park point, since x_{1,sf_2} is inside the stability region of nominal equilibrium point and inside the set D (i.e $x_{1,sf_2} \in \Omega \cap D$) as well. $x_{1,sf_2} \in \Omega \cap D$ ensures that the non-vanishing disturbance caused by safe-parking of CSTR-1 can be rejected in CSTR-2 while $x_{1,sf_2} \in \Omega$ ensures that nominal operation in CSTR-1 can be resumed upon fault repair, as demonstrated by the solid

line in Fig.4.4. In summary, the proposed safe-parking framework provides guidelines to choose safe-park point such that during fault rectification nominal operation in downstream units can be maintained and upon fault repair (at time $t = 9$ hrs), nominal operation of the faulty unit can be resumed.

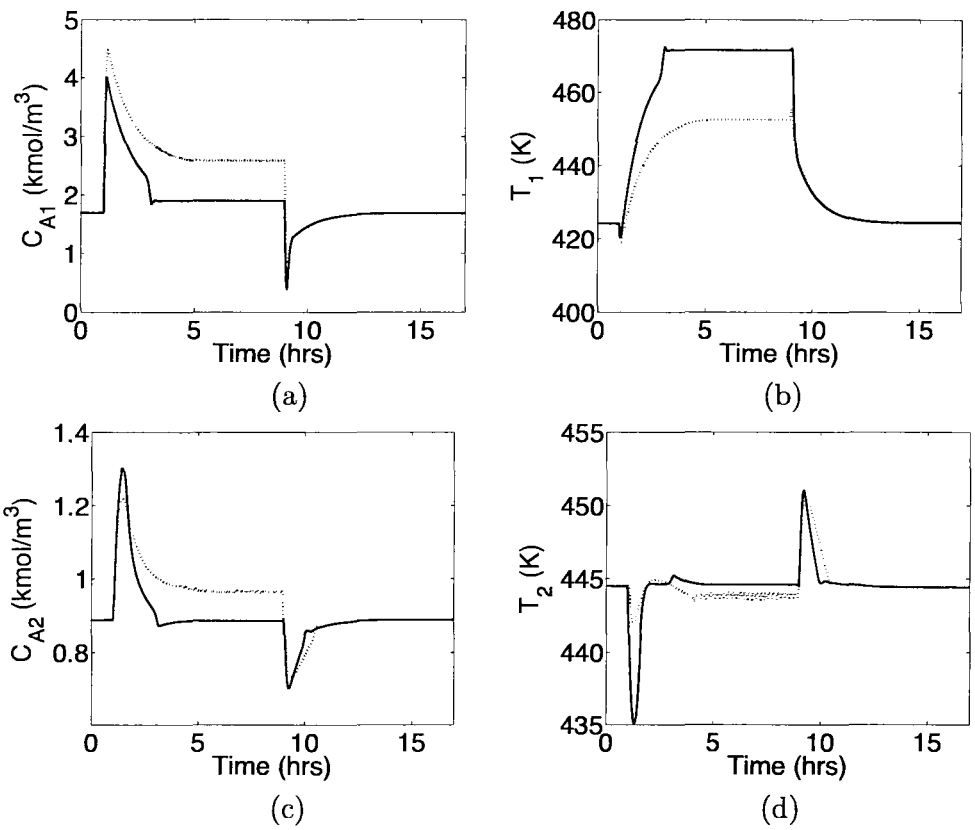


Figure 4.4: Evolution of the closed–loop state profiles of CSTR-1 (a,b) and CSTR-2 (c,d) for the simulation example. Fault occurs at 1 hr and is rectified at 9 hr. Dotted lines ($\cdots$) indicate the case when x_{1,sf_1} (an acceptable safe-park point for the isolated unit) is chosen as the safe-park point for CSTR-1 (resulting in inability to maintain nominal operation in CSTR-2) while the solid lines (—) show the case when x_{1,sf_2} is chosen using the proposed framework as the safe-park point for CSTR-1 (which allows nominal operation in CSTR-2).

Next, we consider the fault scenario, when there is no candidate safe-park point

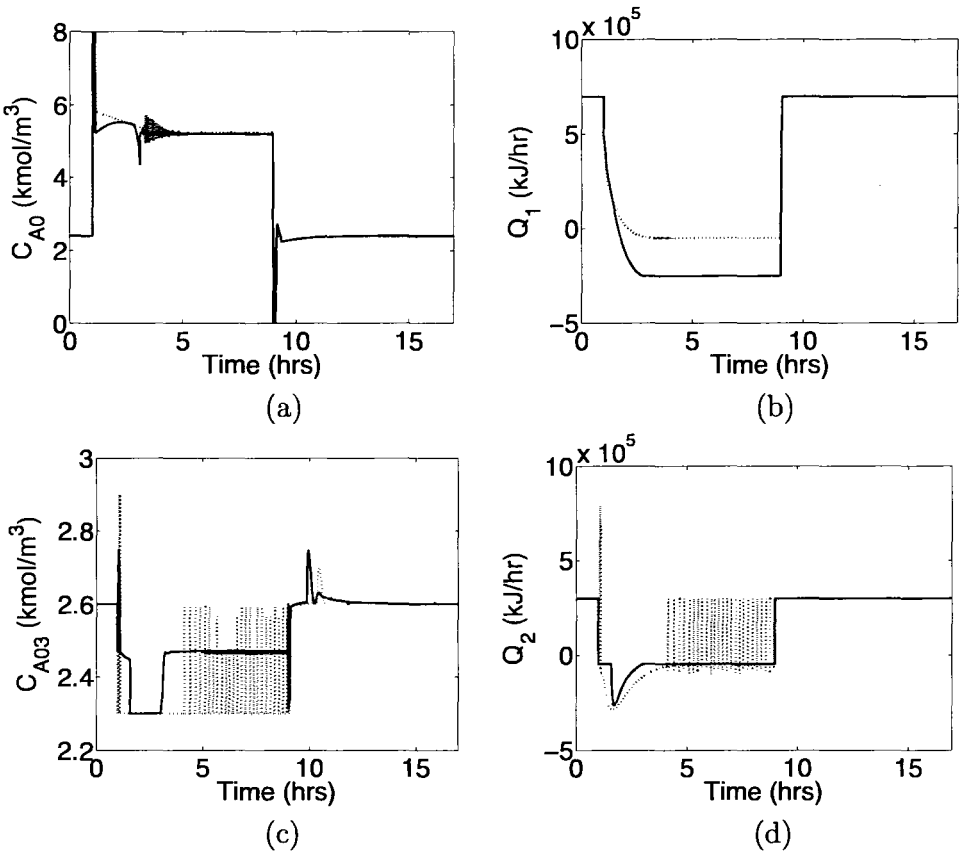


Figure 4.5: Input profiles for CSTR-1 (a,b) and CSTR-2 (c,d) in the simulation example. Fault occurs at 1 hr and is rectified at 9 hr. Dotted lines ($\cdots$) indicate the case when x_{1,sf_1} is chosen as the safe-park point for CSTR-1 while the solid lines (—) show the case when x_{1,sf_2} is chosen as the safe-park point for CSTR-1.

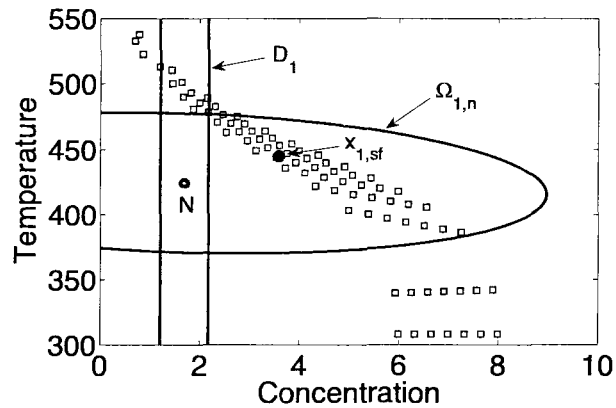


Figure 4.6: Stability region for nominal equilibrium point ($\Omega_{1,n}$), the set D_1 and candidate safe-park points (□) for failure value of C_{A0} for CSTR-1. It can be seen that none of the candidate safe-park point satisfies the conditions in Theorem 4.2, thereby requiring simultaneous safe-parking of the units using Theorem 4.3.

inside $\Omega \cap D$ and thus, there is no safe-park point that can allow continued nominal operation in downstream unit (see Section 4.3.3). To this end, consider a case where a fault occurs in upstream of CSTR-1 restricting the concentration of inlet stream to $6 \leq C_{A0} \leq 8$ kmol/m^3 instead of $0 \leq C_{A0} \leq 8$ kmol/m^3. This fault makes it impossible to continue nominal operation in CSTR-1 because nominal equilibrium point is not an equilibrium point in the faulty scenario. The robust predictive controller for both CSTR's is designed and the stability region for CSTR-2 ($\Omega_{2,N}$) is estimated using $\theta_{min} = -d_{max}$ and $\theta_{max} = d_{max}$ in Eq.3.7. For the simulations we design the robust predictive controller for CSTR-2 using $\theta_{max} = (0.2$ kmol/m^3, 20 K). The stability region for nominal operating point and the set D_k as well as the set of equilibrium points in faulty scenario are shown in Fig.4.6. From Fig.4.6, it can be seen that there exist no candidate safe-park point such that $x_{1,sf} \in \Omega \cap D_k$ and hence, there exists no safe-park point for CSTR-1 such that nominal operation in CSTR-2 can be continued. This requires that both CSTR-1 and CSTR-2 be safe-parked simultaneously. Out of

the safe-park candidates, we choose $x_{1,sf}$: (C_{A1} = 3.59 kmol/m^3, T_1 = 445.0 K) as the safe-park point for CSTR-1, and $x_{2,sf}$: (C_{A2} = 1.30 kmol/m^3, T_2 = 437.3 K) as safe-park point for CSTR-2. As can be seen from the dotted lines in Fig.4.6 (the corresponding state and input profiles are shown as dotted lines in Fig.4.7 and Fig.4.8, respectively) safe-parking of both CSTR's and subsequent resumption of nominal operation (at time t = 9 hrs) is achieved.

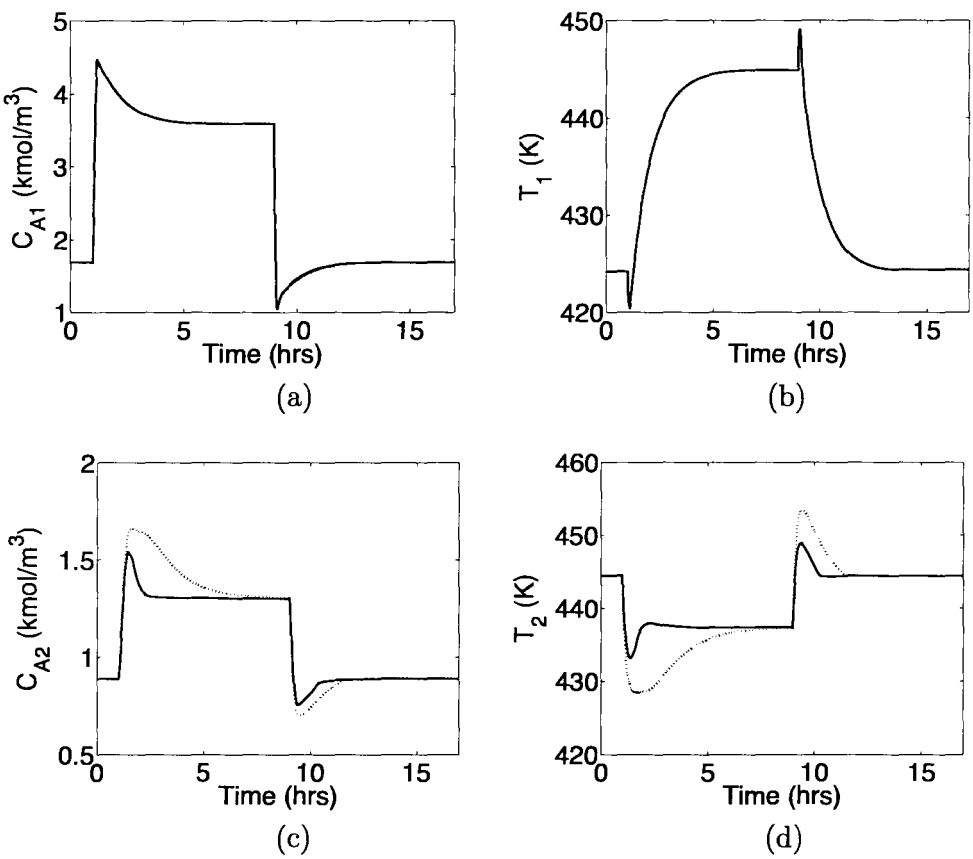


Figure 4.7: Evolution of the closed-loop state profiles of CSTR-1 (a,b) and CSTR-2 (c,d). Fault occurs at 1 hr and is rectified at 9 hr. Dotted lines ($\cdots$) indicate the case when disturbance is considered as unmeasured while the solid lines (—) show the case when disturbance information is passed to the predictive controller of CSTR-2 resulting in improved performance.

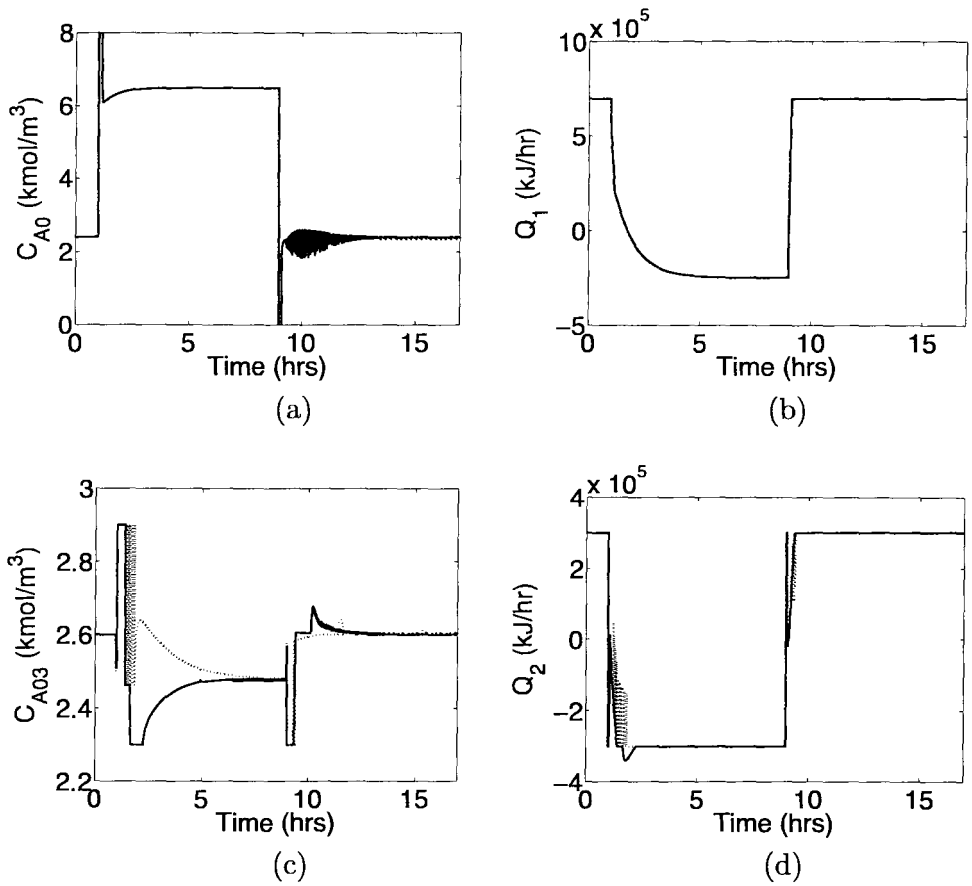


Figure 4.8: Input profiles for CSTR-1 (a,b) and CSTR-2 (c,d). Fault occurs at 1 hr and is rectified at 9 hr. Dotted lines (· · ·) indicate the case when disturbance is considered as unmeasured while the solid lines (—) show the case when disturbance information is passed to the predictive controller of CSTR-2.

Finally, we demonstrate the improvement in performance when the measured values of the process states of CSTR-1 are used in computing the control action in CSTR-2 (instead of the worst case bounds, as described in Remark 4.8). Specifically, the expected state trajectory computed by the predictive controller in CSTR-1 is passed to the controller for CSTR-2. The controller for CSTR-2, therefore, does not use worst-case bounds of the disturbances, but the predicted (and known/measured) values of the process states of CSTR-1. The results are shown by the solid lines in Figs 4.6–4.8, where the improved performance is clearly visible. In particular, we see significantly less overshoot in the temperature and concentration of CSTR-2 both when safe-parking CSTR-2 and when resuming nominal operation in CSTR-2.

4.5 Conclusions

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

Bibliography

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.

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

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.

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

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

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

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

N. H. El-Farra, A. Gani, and P. D. Christofides. Fault-tolerant control of process systems using communication networks. *AIChE J.*, 51:1665–1682, 2005.

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.

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.

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

N. Huynh and N. Kazantzis. Parametric optimization of digitally controlled nonlinear reactor dynamics using zubov-like functional equations. *J. Math. Chem.*, 38:499–519, 2005.

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

I. Karafyllis and C C. Kravaris. Robust output feedback stabilization and nonlinear observer design. *Syst. & Contr. Lett.*, 54:925–938, 2005.

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

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.

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

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.

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

P. Mhaskar. Robust model predictive control design for fault-tolerant control of process systems. *Ind. & Eng. Chem. Res.*, 45:8565–8574, 2006.

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.

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.*, 55:650–659, 2006a.

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, 2006b.

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.

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

C. Panjapornpon and M. Soroush. Shortest-prediction-horizon non-linear model-predictive control with guaranteed asymptotic stability. *Int. J. Contr.*, 80:1533–1543, 2007.

A. C. Raich and A. Cinar. Multivariate statistical methods for monitoring continuous processes: Assessment of discrimination power of disturbance models and diagnosis of multiple disturbances. *Chemom. & Int. Lab. Sys.*, 30:37–48, 1995.

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

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.

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

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.

S. Y. Yoon and J. F. MacGregor. Fault diagnosis with multivariate statistical models part I: using steady state fault signatures. *J. Proc. Contr.*, 11:387–400, 2001.

X. D. Zhang, T. Parisini, and M. M. Polycarpou. Adaptive fault-tolerant control of nonlinear uncertain systems: An information-based diagnostic approach. *IEEE Trans. Automat. Contr.*, 49:1259–1274, 2004.

Blank Page

Chapter 5

Safe-Parking of a Styrene Polymerization Process [†]

5.1 Introduction

Polymerization processes are an important class of chemical processes. The plastic consumption of the world was estimated to be around 200 million tons in 2000 (Rosato et al. [2001]) and continues to grow at a substantial rate. Continuous polymerization reactors are widely used to produce synthetic polymer products such as styrene. The increasing demand for high quality polymers has given impetus to controller designs that provide good control of the polymer product properties and minimize off-spec product during the start-up and the grade transitions. As with most chemical processes, polymerization reactors are characterized by the presence of process nonlinearity, uncertainty and constraints. Over and above the inherent complexity of the process, operation has to deal with eventualities such as equipment and control

[†]The results in this chapter are published in "R. Gandhi, D. Baldwin and P. Mhaskar, Safe-Parking of a Styrene Polymerization Process, *Ind. Eng. Chem. Res.*, 48 (15), 7205-7213, 2009".

algorithm faults, which, if not addressed in a timely manner, can lead to substantial economic losses and safety hazards motivating significant research on fault-tolerant control.

In recent years, there has been a great deal of interest in living chain radical polymerization due to its ability to produce polymers in which the presence (or absence) of branches, number of functional groups (a characteristic of ionic polymerization) and the molecular weight distributions can be properly controlled. In polymer chemistry, the living polymerization is a form of addition polymerization where the ability of a growing polymer chain to terminate has been removed and this is accomplished in a variety of ways. Chain termination and chain transfer reactions are absent and the rate of chain initiation is also much larger than the rate of chain propagation. The result is that the polymer chains grow at a more constant rate than seen in the traditional chain polymerization and their lengths remain very similar (i.e., they have a very low polydispersity index). Though there has been a lot of research effort focused on the understanding of the chemistry of the living chain polymerization, the process system engineering aspects of the process, imperative for successful commercialization, are less explored.

Successful commercialization of any process, apart from profitability and feasibility, requires that process be safe and operable despite disturbances and faults in industrial environment. In this chapter, we design control strategy to control living chain polymerization reactor at an unstable operating point using Lyapunov based MPC and address the problem of how to operate the reactor during fault-rectification for the faults that do not allow continuation of nominal operation in the reactor. First

we design a Lyapunov based predictive controller for the styrene polymerization reactor in a way that allows for an explicit characterization of the set of initial conditions from where the reactor can be stabilized. Then, we consider the problem of handling faults in the manipulated inputs. We design and implement the safe-parking framework to choose a safe-park point where the reactor can be operated during fault rectification. Upon fault recovery, the process states are driven back to the nominal operation. This ensures safe-operation and minimizes deviation from specs during fault rectification and smooth resumption of nominal operation upon fault recovery.

The rest of the chapter is organized as follows: In Section 5.2, the styrene polymerization process is described and a mathematical model for the process is presented. Next we describe the control objectives for the styrene polymerization reactor. A Lyapunov-based predictive controller is designed in Section 5.3.1 and implemented in Section 5.3.2. Next, in Section 5.4.2 a safe-parking framework is designed and used to handle faults in Section 5.4.3. Finally we summarize our results in Section 5.5.

5.2 Process description and modeling

A schematic of a typical styrene polymerization reactor setup is shown in Fig. 5.1. Living Nitroxide-Mediated Radical Polymerization (NMRP) of styrene takes place in the CSTR. We consider the scenario where Monomer feed to the CSTR comes from two different sources, through intermediate storage tanks, Tank-1 and Tank-2. Nitroxyl ether is fed to the CSTR to keep the ratio of total monomer feed to nitroxyl ether constant. In Bonilla et al. [2002] and Lemoine-Nava et al. [2006], a detailed kinetic mechanism for the NMRP of styrene via manomolecular process is

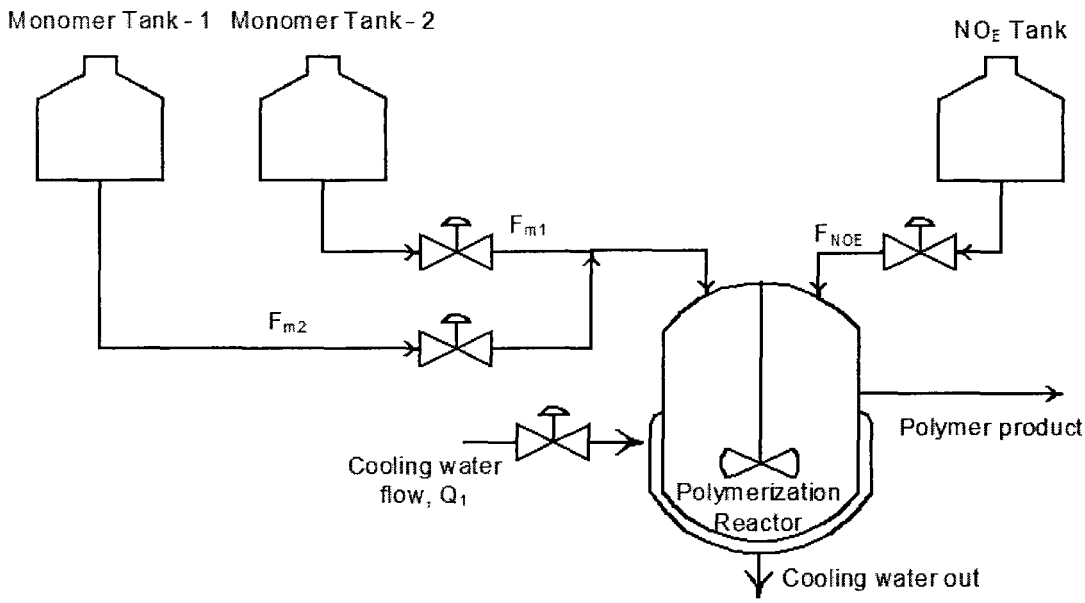


Figure 5.1: Schematic of the Living Nitroxide-Mediated Radical Polymerization reactor.

reported (reproduced in Table 5.1 for convenience). The numerical values of the activation energy and pre-exponential factors in Arrhenius-like rate constant equations are provided in Table 5.2.

Table 5.1: NMRP living polymerization kinetic scheme

Nitroxyl ether decomposition	$NO_E \underset{k_{d2}}{\overset{k_{a2}}{\leftrightarrow}} R^{\cdot} + NO_x^{\cdot}$
Mayo dimerization	$M + M \overset{kdim}{\leftrightarrow} D$
Thermal initiation	$D^{+} \overset{k_i}{\leftrightarrow} \dot{M} + \dot{D}$
First propagation (primary radicals)	$\dot{R} + M \overset{k_p}{\leftrightarrow} \dot{P}_1$
First propagation (monomeric radicals)	$\dot{M} + M \overset{k_p}{\leftrightarrow} \dot{P}_1$
First propagation (dimeric radicals)	$\dot{D} + M \overset{k_p}{\leftrightarrow} \dot{P}_1$
Propagation	$\dot{P}_n + M \overset{k_p}{\leftrightarrow} \dot{P}_{n+1}$
Dormant-living exchange (monomeric alkoxyamine)	$\dot{M} + \dot{NO}_x \underset{k_a}{\overset{k_d}{\leftrightarrow}} MON_x$
Dormant-living exchange (polymeric alkoxyamine)	$\dot{P}_n + \dot{NO}_x \underset{k_a}{\overset{k_d}{\leftrightarrow}} P_nON_x$
Alkoxyamine decomposition	$MONx \overset{k_{decomp}}{\leftrightarrow} M + HON_x$
Rate enhancement reaction	$D + \dot{NO}_x \overset{k_{h3}}{\leftrightarrow} \dot{D} + HON_x$
Termination by combination	$\dot{P}_n + \dot{P}_m \overset{k_{tc}}{\leftrightarrow} D_n + D_m$
Termination by disproportionation	$\dot{P}_n + \dot{P}_m \overset{k_{td}}{\leftrightarrow} D_n + D_m$
Transfer to monomer	$\dot{P}_n + M \overset{k_{trm}}{\leftrightarrow} \dot{M} + D_n$
Transfer to dimer	$\dot{P}_n + D \overset{k_{trd}}{\leftrightarrow} \dot{D} + D_n$

Table 5.2: NRMP living polymerization kinetic information

Parameter	Value	Unit
k_i	$e^{(7.0233\ e-7616.7/T)}$	L/(mols)
k_{dim}	$10^{4.4}\ e^{(-93.5/RT)}$	L/(mols)
k_p	$10^{7.63}\ e^{(-32.51/RT)}$	L/(mols)
k_{tc}	$1.7 \times 10^9\ e^{-843/T}$	L/(mols)
k_{td}	0	L/(mols)
k_{trm}	0	L/(mols)
k_{trd}	0	L/(mols)
k_{decomp}	$5.7 \times 10^{14}\ e^{-153/RT}$	L/s
k_{h3}	0.1	L/(mols)
k_d	$4.7 \times 10^9 e^{-9.6296/RT}$	L/(mols)
k_a	$3 \times 10^{13}\ e^{-124/RT}$	L/s
k_{d2}	k_d	L/(mols)
k_{a2}	k_a	L/s

Table 5.3: Design parameters and thermodynamic information

Design Parameter	**Value**	**Unit**
Monomer feed stream concentration	8.7	mol/L
Nitroxyl ether feed stream concentration	0.0087	mol/L
Feed stream flow rate	0.372	L/s
Feed stream temperature	403.15	K
Cooling water flow rate	1	L/s
Cooling water feed temperature	293.15	K
Reactor volume	9450	L
Cooling jacket volume	2000	L
Heat transfer coefficient	80	J/(m^{2}sK)
Heat transfer area	19.5	m^2
Heat of reaction	-73000	J/mol
Feed stream heat capacity	1647.27	J/(kgK)
Cooling water heat capacity	4045.7	J/(kgK)
Feed stream density	0.915	kg/L
Cooling water density	1	kg/L

5.2.1 Styrene polymerization reactor model

We utilize the mathematical model derived in Verazaluce-Garcia et al. [2000] and Lemoine-Nava et al. [2006], reproduced below:

$$\frac{dM}{dt} = \frac{(M_{in} - M)}{\theta} - 2k_{dim}M^2 - k_i DM - k_p M(\dot{D} + \dot{M} + \dot{R}) - k_p MY_o - k_{trm}MY_o + k_{decomp}MON_x \quad (5.1)$$

$$\frac{dD}{dt} = -\frac{D}{\theta} + k_{dim}M^2 - k_i DM - k_{trd}DY_o - k_{h_3}DNO_x \quad (5.2)$$

$$\frac{dNO_E}{dt} = \frac{(NO_{E,0} - NO_E)}{\theta} - k_{a_2}NO_E + k_{d_2}NO_x\dot{R} \quad (5.3)$$

$$\frac{d\dot{M}}{dt} = -\frac{\dot{M}}{\theta} + k_i DM - k_p M\dot{M} - k_d NO_x\dot{M} + k_a MON_x + k_{trm}MY_o \quad (5.4)$$

$$\frac{d\dot{R}}{dt} = -\frac{\dot{R}}{\theta} - k_p\dot{R}M + k_{a_2}NO_E - k_{d2}\dot{R}NO_x \quad (5.5)$$

$$\frac{d\dot{D}}{dt} = -\frac{\dot{D}}{\theta} + k_i DM - k_p\dot{D}M + k_{trd}DY_o + k_{h_3}DNO_x \quad (5.6)$$

$$\frac{dNO_x}{dt} = -\frac{NO_x}{\theta} - k_d NO_x Y_o + k_a Z_o + k_{a_2}NO_E - k_d NO_x\dot{M} + k_a MON_x - k_{d2}NO_x\dot{R} - k_{h_3}DNO_x \quad (5.7)$$

$$\frac{dMON_x}{dt} = -\frac{MON_x}{\theta} + k_d NO_x\dot{M} - k_a MON_x - k_{decomp}MON_x \quad (5.8)$$

$$\frac{dY_o}{dt} = -\frac{Y_o}{\theta} + k_p M(\dot{D} + \dot{M} + \dot{R}) + k_a Z_o - Y_o(k_d NO_x + k_{trm}M + k_{trd}D + (k_{tc} + k_{td})Y_o) \quad (5.9)$$

$$\frac{dZ_o}{dt} = -\frac{Z_o}{\theta} + k_d NO_x Y_o - k_a Z_o \quad (5.10)$$

$$\frac{dT}{dt} = \frac{(Tin - T)}{\theta} + \frac{((-\Delta H)kpM(\dot{M} + \dot{R} + \dot{D} + Y_o))}{(\rho C_{pm})} - \frac{(UA(T - T_j))}{(\rho C_{pm}V_j)} \quad (5.11)$$

$$\frac{dT_j}{dt} = \frac{Q_w}{V_j}(T_{j,in} - T_j) + \frac{(UA(T - T_j))}{(\rho C_{pm}V_j)} \quad (5.12)$$

$$\frac{dY_1}{dt} = -\frac{Y_1}{\theta} + k_p M(\dot{D} + \dot{M} + \dot{R}) + k_a Z_1 + k_p MY_o - Y_1(k_d NO_x + k_{trm}M + k_{trd}D + (k_{tc} + k_{td})Y_o) \quad (5.13)$$

$$\frac{dY_2}{dt} = -\frac{Y_2}{\theta} + k_p M(\dot{D} + \dot{M} + \dot{R} + Y_o + 2Y_1) + k_a Z_2 - Y_2\,(k_d NO_x + k_{trm}M + k_{trd}D + (k_{tc} + k_{td})Y_o) \quad (5.14)$$

$$\frac{dZ_1}{dt} = -\frac{Z_1}{\theta} + k_d NO_x Y_1 - k_a Z_1 \quad (5.15)$$

$$\frac{dZ_2}{dt} = -\frac{Z_2}{\theta} + k_d NO_x Y_2 - k_a Z_2 \quad (5.16)$$

$$\frac{dQ_o}{dt} = -\frac{Q_o}{\theta} + (\frac{1}{2}k_{tc} + k_{td})Y_o^2 + Y_o(k_{trm}M + k_{trd}D) \quad (5.17)$$

$$\frac{dQ_1}{dt} = -\frac{Q_1}{\theta} + (k_{tc} + k_{td})Y_1 Y_o + Y_1(k_{trm}M + k_{trd}D) \quad (5.18)$$

$$\frac{dQ_2}{dt} = -\frac{Q_2}{\theta} + (k_{tc} + k_{td})Y_o Y_2 + k_{tc}Y_1^2 + Y_2(k_{trm}M + k_{trd}D) \quad (5.19)$$

where M is monomer concentration, D is dimer concentration, NO_E is nitroxyl ether concentration, $\dot{M}$ is monomer radical concentration, $\dot{R}$ is primary radical concentration, $\dot{D}$ is dimer radical concentration, NO_x is nitroxide concentration, MON_x is

alkoxyamine concentration, T is reactor temperature, T_j is jacket water temperature, Q_w is cooling water flowrate to jacket, M_{in} is concentration of monomers in feed, V is the volume of the reactor, Q is total volumetric flowrate fed to reactor and $\theta = \frac{V}{Q}$. A material balance for the species and polymer moments in the styrene polymerization reactor gives Eqs.5.1-5.10 and Eqs.5.13-5.19. An energy balance for both the reactor and the cooling jacket gives Eqs.5.11-5.12. The evolution of the process state of the reactor is governed by 12 equations i.e. Eqs.5.1-5.12. The rest of the model equations are required to calculate the end product quality measures such as average molecular weight and polydispersity. The values of the design parameters for the reactor and the thermodynamic properties are shown in Table 5.3. The polymer end properties such as average number molecular weight (M_n), average weight molecular weight (M_w) and polydispersity are calculated using Eqs.5.20-5.22.

$$M_n = MW_M \frac{Z_1 + Q_1 + Z_1}{Z_0 + Q_0 + Z_0} \tag{5.20}$$

$$M_w = MW_M \frac{Z_2 + Q_2 + Z_2}{Z_1 + Q_1 + Z_1} \tag{5.21}$$

$$\text{Polydispersity} = \frac{M_w}{M_n} \tag{5.22}$$

where MW_M is the monomer molecular weight (104.16 g/mol).

5.2.2 Control strategy

In this section, we briefly explain the control objectives and the control strategy for the styrene polymerization reactor. The control objective is to ensure production of desired end quality, defined via the quality measures such as average molecular weight and polydispersity. The manipulated variables for achieving this objective are

monomer feed flowrate and cooling water flowrate. To facilitate controller design, the process model of Eqs.5.1-5.22 can be divided into three groups as follows.

$$\dot{x} = f(x) + g(x)u \tag{5.23}$$

$$\dot{z} = l(x, z) \tag{5.24}$$

$$y = h(x, z) \tag{5.25}$$

where $x = [M,\ D,\ NO_E,\ \dot{M},\ \dot{R},\ \dot{D},\ NO_x,\ MON_x,\ Y_o,\ Z_o,\ T,\ T_j]^T$ is the vector of state variables, $u = [M_{in}, Q_w]^T$ is the vector of manipulated inputs, $z = [Y_1,\ Y_2,\ Z_1,\ Z_2,\ Q_o,\ Q_1,\ Q_2]^T$ is the vector of output variables and $y = [M_n,\ M_w,$ Polydispersity $]^T$ are the quality variables. The control objective is to stabilize the process at the desired values of process states, chosen to yield the desired product quality indicators; furthermore, for the sake of illustration, an average molecular weight in the range $20,000 - 22,000$ gm/mol and the polydispersity in the range $2.7 - 2.9$ is deemed acceptable.

Note that the polymerization reaction exhibits heat balance multiplicity and there can be one or three equilibrium points depending on the values of the process parameters. Where multiple equilibrium points exist, the equilibrium points corresponding to the upper and lower temperatures are stable while the equilibrium point corresponding to the middle temperature is unstable. Unlike a typical reaction, the reaction rate in polymerization reactor does not increase monotonically with the temperature due to gel effects in the reactor at higher conversions. To attain optimal reaction rate in the reactor, therefore, the reactor is operated at mid-range temperatures, resulting in the need to operate the process at an unstable equilibrium point (denoted by N). The

physical limitations in the process design imposes the following constraints on the manipulated variables; the constraints for the monomer feed flowrate is $0 \leq Q \leq 0.8$ L/s and for the cooling water flowrate is $0 \leq Q_w \leq 5$ L/s. The steady state values of the state variables corresponding to the nominal values of the manipulated variables $Q_w = 1$ L/s and $Q = 0.52$ L/s are given in Table 5.5.

5.3 Lyapunov-based model predictive control of the polymerization reactor

In this section, we design and implement a recently developed Lyapunov-based predictive controller on the polymerization reactor. The key benefit of the predictive control design is that it possesses an explicitly characterized set of initial conditions from where it is guaranteed to be feasible, and hence stabilizing in the presence of input constraints.

5.3.1 Controller design

Consider the system of Eq.5.23 for which we design a predictive controller (Mhaskar et al. [2005]) of the form:

$$u_1(\cdot) = argmin\{J(x,t,u(\cdot))|u(\cdot) \in S\} \tag{5.26}$$

$$s.t.\ \dot{x} = f(x) + G(x)u(t) \tag{5.27}$$

$$\dot{V}(x(\tau)) \leq -\epsilon^* \ \forall\, \tau \in [t, t+\Delta)\ if\ \ V(x(t)) > \delta' \tag{5.28}$$

$$V(x(\tau)) \leq \delta' \ \forall\, \tau \in [t, t+\Delta)\ \ if\ \ V(x(t)) \leq \delta' \tag{5.29}$$

$$x(t+\tau) \in \Pi^+ \; \forall \, \tau \in [t, t+\Delta) \; if \; V(x(t)) > c^{max^+} \tag{5.30}$$

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 (with $N_{MPC} = T/\Delta$. Eq.5.27 is the nonlinear model describing the time evolution of the state x, V is a control Lyapunov function and δ', ϵ^* are controller parameters. The parameters c^{max^+} and the set Π^+ are defined below. A control $u(\cdot)$ in S is characterized by the sequence $\{u[j]\}, j = 0 \ldots N_{MPC} - 1$. The performance index is given by

$$J(x,t,u(\cdot)) = \int_t^{t+T} \left[\|x^u(s;x,t)\|^2_{Q_w} + \|u(s)\|^2_{R_w} \right] ds \tag{5.31}$$

where Q_w is a positive semi-definite symmetric matrix and R_w is a strictly positive definite symmetric matrix. $x^u(s;x,t)$ denotes the solution of Eq.5.23, due to control u, with initial state x at time t. The minimizing control $u[0] \in S$ is then applied to the plant over the interval $[t, t+\Delta)$ and the procedure is repeated indefinitely.

For all values of the styrene polymerization process, negative definiteness of the Lyapunov function derivative can be achieved subject to manipulated input constraints (and independent of the control law) in the set described by:

$$\Pi^+ = \{x \in \mathbb{R}^n : L_f V(x) + \sum_{i=1}^{m} L_{G_i^{min}} V(x) u^i \leq -\epsilon^{**}\} \tag{5.32}$$

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 (appropriately defined, and related to ϵ^* through the sampling time Δ; see Mahmood and Mhaskar [2008] for details). The set Π^+ therefore denotes the entire set of initial conditions from where $\dot{V} < -\epsilon^{**}$ is achievable. The idea behind the expression in Eq.5.32 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 $|u_{max}^i| = |u_{min}^i| = u_i^{norm}$) where $sgn(x) = 1$ if $x \geq 0$ and $sgn(x) = -1$ if $x < 0$. Subsequently, computation of the largest level set Ω^+, of the form

$$\Omega^+ = \{x \in \mathbb{R}^n : V(x) \leq c^{max^+}\} \tag{5.33}$$

completely contained in Π^+ provides an estimate of the stability region. For further details on the controller design and a stability proof, see Mahmood and Mhaskar [2008].

Remark 5.1. The Lyapunov based predictive controller of Eqs.5.26–5.31 guarantees stability from all initial conditions inside set Ω^+. If the process states are initially outside the set Ω^+ but inside the set Π^+ then the constraints in the predictive controller formulation requiring that process states remain inside the set Π^+ allows to possibly enhance the set of initial conditions from where the process can be stabilized. Given the high dimensional nature of the problem, and the possible conservatism associated with utilizing quadratic Lyapunov functions (which are easy to construct) this constraint provides further assurance that the controller will be able to recover from a disturbance that throws it away from nominal operation.

5.3.2 Controller implementation

We now implement the Lyapunov-based predictive controller on the styrene polymerization reactor. The Lyapunov-based model predictive controller minimizes a quadratic cost function subject to input and stability constraints. Note that for the controller design, we utilize a quadratic Lyapunov function of the form $V = x^T P x$, where P is positive definite matrix calculated by solving the Riccati equality of Eq.2.2. The stability guarantees however, explicitly account for the nonlinear process model. Prediction and control horizons of 100 sec are used for the controller design and implementation. A discretized version of the stability constraint of the form $V(x(t+\Delta)) \leq 0.99V(x(t))$ is incorporated in the MPC optimization problem.

We tested the controller implementation from several initial conditions. Shown here is the simulation result for a cold filled start-up of the polymerization reactor where the polymerization is started from an initial condition $M_n = 8$ mol/L, $T = 300$ K and $T_j = 300$ K while all the other concentrations start at zero. As can be seen in the Fig. 5.2, the Lyapunov based predictive controller is able to stabilize the process at the desired unstable operating point. Fig. 5.3 shows the corresponding input profiles. Fig. 5.4 shows the evolution of the Lyapunov function and it can be seen that the Lyapunov function continuously decreases, driving the process towards the desired operating point.

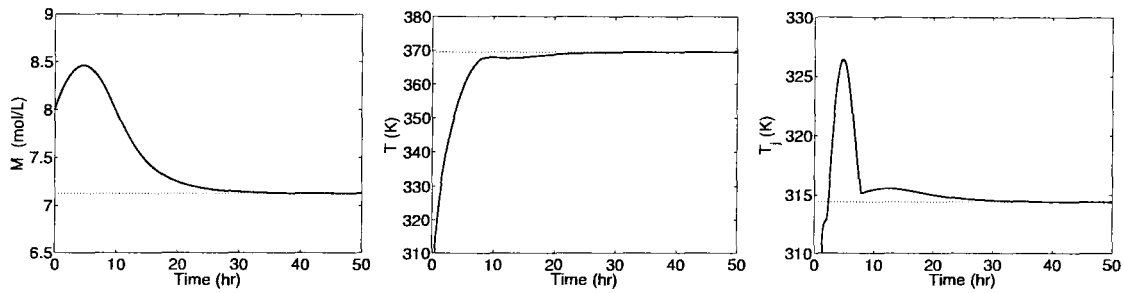


Figure 5.2: State profile evolution (solid lines) for the stabilization of the styrene polymerization process from a cold startup to the desired unstable equilibrium point (a) Monomer concentration (M), (b) Reactor Temperature (T), and (c) Jacket Temperature (T_j). The dotted lines denote the desired steady-state values.

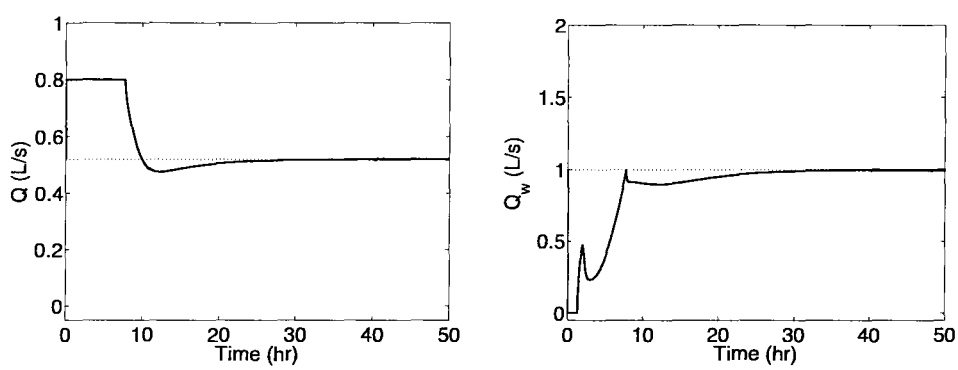


Figure 5.3: Input profile for the stabilization of the styrene polymerization process from a cold startup to the desired unstable equilibrium point (a) Inlet monomer flowrate (Q), and (b) Jacket cooling water flowrate (Q_w). The dotted lines denote the nominal values of the manipulated inputs.

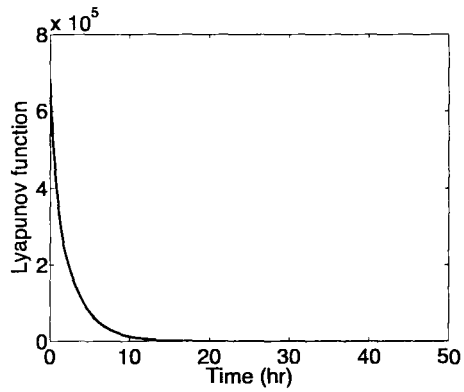


Figure 5.4: Lyapunov function evolution for the stabilization of the styrene polymerization reactor process from a cold startup to the desired unstable equilibrium point.

5.4 Handling faults in the operation of the polymerization reactor

In this section, we design a framework for handling actuator faults in the polymerization process. To this end, first we formulate the problem and then design and implement a safe-parking framework Chapter 2 on the polymerization process.

5.4.1 Problem statement

We illustrate the safe-parking mechanism by considering a fault scenario where the valve regulating the flow from one of the monomer tanks (tank-1) fails and reverts to its fail safe (completely shut) position. This results in modified constraints on the monomer feed flow rate $0 \leq Q \leq 0.4$ L/s. As the nominal operating point corresponds to $Q = 0.52$ L/s, no value of the functioning manipulated inputs $0 \leq Q_w \leq 5$ L/s and $0 \leq Q \leq 0.4$ L/s exists such that the nominal equilibrium point (N) continues to be an equilibrium point of the process subject to the fault. This requires that the process

be shutdown or be taken to some other operating point that is an equilibrium point for the allowable values of the manipulated variable in the faulty scenario. In this chapter, we use the safe-parking framework that systematically selects a temporary operating point so that the process can be safely operated during fault rectification and upon fault recovery nominal operation can be efficiently resumed. The selection of the temporary operating point is made such that the polymer product during fault rectification has quality close to the desired product quality.

5.4.2 Safe-parking framework

For the styrene polymerization reactor, consider a fault scenario described in Section 5.4.1 where the monomer feed from one of the feed tanks is lost due to a fault in the feed unit. The fault takes place at time T^{fault} and is repaired at time T^{repair}. Maintaining $Q_w = 1$ L/s and $Q = 0.4$ L/s (maximum possible value for monomer feed flowrate) may drive the process state to a point from where it may not be possible to resume the nominal operation upon fault-repair, or even if possible, may yield significantly off-spec product (see the simulation section for a demonstration). Furthermore, even if the output variables can be maintained close to specs during fault repair, it is important to ensure resumption of nominal operation especially in the context of a plant setting where the outlet from the unit goes into another processing unit, and resuming nominal operation of the entire state variables (not just the quality variables) is necessary to minimize disruptions downstream.

For the allowable ranges of inputs $0 \leq Q_w \leq 5$ L/s and $0 \leq Q \leq 0.4$ L/s, a set of equilibrium points where the process can be stabilized during fault rectification can be calculated and is denoted as the candidate safe-park set, $X_c := \{x_c \in \mathbb{R}^n :$

$f(x_c) + g(x_c)u = 0,\ 0 \leq Q_w \leq 5$ L/s, $\ 0 \leq$ Q ≤ 0.4 L/s$\}$. The safe-park candidates therefore represent the equilibrium points at which the unit can be stabilized, subject to the failed actuator, and with the other manipulated variables within the allowable ranges.

Arbitrarily choosing a temporary operating point $x_s \in X_c$ (as with trying to run the monomer feed at the maximum residual flow rate), may yield significantly off-spec product during fault-rectification, motivating the need to implement the safe-parking framework. The key requirements for the choice of a safe-park point is that, 1) it should be possible to drive the process to the safe-park point from the nominal equilibrium point, 2) it should be possible to operate the process at the temporary operating point with the allowable values of manipulated variables in faulty scenario, and 3) it should be possible to resume nominal operation after the fault is rectified. These requirements can be satisfied by choosing an operating point such that 1) the process state at the time of failure resides in the stability region of the safe-park candidate (subject to depleted control action), so the process can be driven to the candidate safe-park point and 2) the safe-park candidate resides within the stability region of the nominal control configuration so the process can be returned to nominal operation after fault repair.

These requirements are formalized in Theorem 5.1 below. To this end, consider the fault scenario described earlier where the failure occurs in one of the monomer feed units. The stability region under nominal operation, denoted by Ω_n^+, has been characterized for the model predictive controller of Eqs.5.26–5.31. Similarly, for a candidate safe-park point x_c, we denote Ω_c^+ as the stability region (computed a priori) and $u = u_n$ and $u = u_{x_c}$ are the controllers designed to stabilize the process at the

nominal equilibrium point and the safe-park point, respectively.

Theorem 5.1. [Chapter 2] *Consider the constrained system of Eq.5.23 under the model predictive controller of Eqs.5.26-5.31 designed, for a given positive number* ϵ, *to achieve* $\limsup_{t\to\infty} \|x(t)\| \leq \epsilon$. *If* $x(0) \in \Omega_n^+$, $x(T^{fault}) \in \Omega_c^+$ *and* $\Omega_c^+ \subset \Omega_n^+$, *then the switching rule*

$$u(t) = \left\{ \begin{array}{lll} u_n & , & 0 \leq t < T^{fault} \\ u_{x_c} & , & T^{fault} \leq t < T^{repair} \\ u_n & , & T^{repair} \leq t \end{array} \right\} \tag{5.34}$$

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

Remark 5.2. Note that the assumption that the failed actuator reverts to the fail-safe position allows enumerating the possible fault situations for any given set of manipulated inputs a-priori to determine the safe-park candidates off-line and then pick the appropriate safe-park point online (the condition $x_s \in \Omega_n^+$ can be verified off-line, however $x(T^{fault}) \in \Omega_{x_s}^+$ needs to be verified online, but only requires an algebraic calculation). The assumption reflects the practice wherein actuators have a built-in fail-safe position to which they revert upon failure. The fail-safe positions are typically determined to minimize the possibility of excursion 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). In the unlikely event that the actuators experience a mechanical failure and are not able to revert to a fail-safe position, one can work with simplified (albeit without guarantees) estimates of the stability regions that can be generated much faster (and therefore computed online, upon fault-occurrence), to implement the safe-parking mechanism.

Specifically, instead of stability regions estimated by constructing invariant sets Ω^+ within the set of initial conditions Π^+ for which the Lyapunov-function can be made to decay, one can use the set Π^+ (which is much easier to compute) to implement the safe-park mechanism as is done in this work. Note also that while the statement of Theorem 2 considers faults in one of the actuators, generalizations to multiple faults (simultaneous or otherwise) are possible, albeit involving the expected increase in off-line computational cost (due to the necessity of determining the safe-park points for all combinations of the faults in the control actuators). Note also that while the computational requirements grow with increase in the number of states and inputs, the majority of the computations are off-line and require only algebraic computations.

Remark 5.3. The presence of constraints on the manipulated inputs limits the set of initial conditions from where the process can be driven to a desired equilibrium point. Control designs that allow an explicit characterization of their stability regions, and their use in deciding the safe-park point is therefore critical in determining the viability of a candidate safe-park point. Note the presence of a point in the stability region can be verified by evaluating the Lyapunov function value. 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 recovery times, and only provides appropriate switching logic that is executed when and if a fault takes place and is subsequently rectified. Note that while not explicitly considered in this chapter, plant-model mismatch and disturbances can be accounted for in the proposed framework. In particular, first a robust MPC must be designed that provides an estimate of the stability region in the presence of uncertainties and then the safe-parking algorithm should be implemented using the robust

stability region estimates (see Chapter 3 for further details). On the other hand, if the measurements are available only asynchronously, there exists a limiting value of measurement loss fraction within which the predictive controller continues to enforce practical stability (see Mhaskar et al. [2007]), and if the sensor data-loss is found to be within the acceptable limit, the predictive controller can be utilized to implement the safe-parking framework.

Remark 5.4. Note that the choice of the control Lyapunov function has an effect on the estimates of the stability region, and, in turn, on the implementation of the proposed safe-parking framework. 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.5.27 is currently not available. Yet, for several classes of nonlinear process systems that arise commonly in the modeling of engineering applications, it is possible to use suitable approximations (Dubljevic and Kazantzis [2002]) or exploit system structure to construct CLFs. The key is for the control design to be able to utilize the CLF to ensure a well defined stability region, which enables the implementation of the proposed safe-parking framework. Note also that implicit in the implementation of the proposed safe-parking mechanism is the assumption of the presence of fault-detection and isolation filters. The proposed safe-parking framework determines the necessary course of action after a fault has been detected and isolated and can be readily integrated with any of the existing (e.g., El-Farra and Ghantasala [2007], Ghantasala and El-Farra [2008], Mhaskar et al. [2008]) fault-detection and isolation structures.

Remark 5.5. Often, a large set of equilibrium points may qualify as safe-park points and satisfy the requirements in Theorem 5.1. In such a scenario, a safe-park point that

is optimal from an economic sense should be chosen as a safe-park point. In Chapter 2, a framework to incorporate the cost (a) for transitioning from the nominal equilibrium point to a safe-park point, (b) for operating the process at a safe-park point and (c) of transitioning from a safe-park point to the nominal equilibrium point after fault is rectified was presented. For the styrene polymerization reactor, when more than one candidate safe-park point is available, the safe-park point which produces polystyrene with the end product qualities closest to the desired product quality is chosen as the safe-park point.

5.4.3 Safe-parking of styrene polymerization reactor

Consider the fault described in Section 5.4.1, where the monomer feed from one of the feed tanks is lost due to a fault in the feed unit. In this faulty scenario, the nominal equilibrium point is no longer an equilibrium point and the process can not be operated at the nominal equilibrium point and needs to be operated at some other operating point. In the absence of the safe-parking framework, one possibility is that even after being informed of the fault, the controller tries to maintain operation at the nominal operating point with available control action. Since the nominal equilibrium point is no longer an equilibrium point in the faulty scenario, the states go to another equilibrium point (as shown by the dashed lines in Fig. 5.5). The corresponding input profile is shown (see dashed lines) in Fig. 5.6. As a result, the product during fault-repair has a number average molecular weight (M_n) of 27073 gm/mol and polydispersity of 4.05 which are significantly away from the desired values and is essentially a waste product.

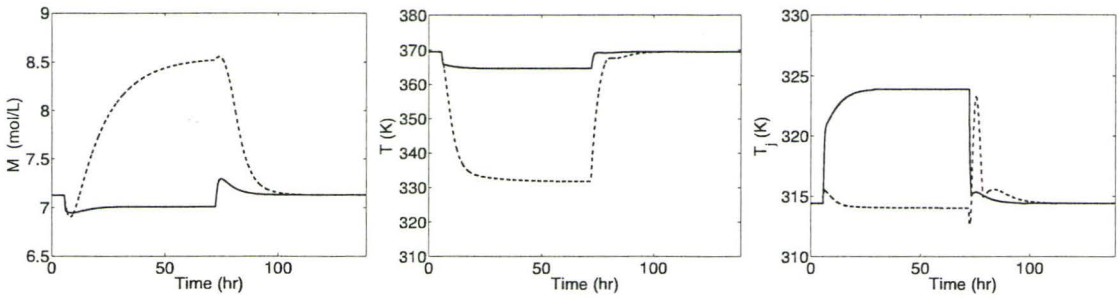
We next demonstrate the scenario when the safe-parking framework of Section

Table 5.4: Candidate safe-park points

No	M (mol/L)	T (K)	Q_w (L/s)	Q (L/s)	M_n (gm/mol)	Poly-dispersity
1	6.668	367.5	0.56	0.34	26226	2.615
2	6.407	368.9	0.56	0.32	29340	2.441
3	7.010	364.6	0.51	0.35	22036	2.981
4	6.198	373.5	0.85	0.38	31732	2.247
5	5.971	373.8	0.74	0.34	34323	2.183
6	5.709	376.1	0.82	0.34	37202	2.088
7	5.398	376.8	0.70	0.30	40541	2.026
8	4.986	381.0	0.85	0.31	44627	1.934
9	4.520	384.8	0.89	0.30	48909	1.872
10	3.689	391.4	0.80	0.27	55469	1.810

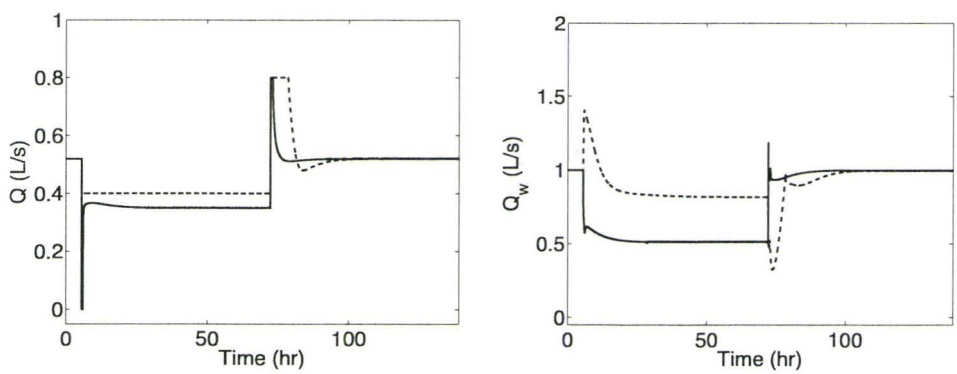
Table 5.5: Values of state variable corresponding to nominal equilibrium point, safe-park point and the equilibrium point where process settles in absence of safe-parking framework

State/property	Units	Nominal Equilibrium point (N)	safe-park point (x_sf)	Controller tries to to maintain nominal operation
M	mol/L	7.13	7.01	8.49
D	mol/L	1.21×10^{-3}	1.13×10^{-3}	1.46×10^{-4}
NO_E	mol/L	3.35×10^{-3}	3.66×10^{-3}	8.33×10^{-3}
$\dot{M}$	mol/L	1.39×10^{-12}	1.14×10^{-12}	5.40×10^{-14}
$\dot{R}$	mol/L	3.82×10^{-11}	2.84×10^{-11}	2.70×10^{-11}
$\dot{D}$	mol/L	1.40×10^{-12}	1.15×10^{-12}	5.43×10^{-14}
No_x	mol/L	3.36×10^{-7}	2.39×10^{-7}	3.63×10^{-7}
MON_x	mol/L	6.66×10^{-7}	6.06×10^{-7}	1.95×10^{-8}
Y_o		1.12×10^{-8}	9.48×10^{-8}	1.50×10^{-9}
Z_o		5.35×10^{-3}	5.04×10^{-3}	3.67×10^{-4}
T	K	369.50	364.57	331.73
T_j	K	323.90	326.74	314.02
Q	L/s	0.52	0.35	-
Q_w	L/s	1.00	0.51	-
Mn	mol/L	20585	22036	27073
Polydispersity		2.81	2.98	4.05



(a) (b) (c)

Figure 5.5: (a) Monomer concentration (M) (b) Reactor Temperature (T), and the (c) Jacket Temperature (T_j) for living chain styrene polymerization reactor. Fault occurs at 5 min and is rectified at 75 min. Dashed lines (- -) show the state profile when the controller tries to maintain nominal operation despite fault in one of the monomer streams and the solid lines (—) show the state profile for the case when the safe-parking framework is implemented.



(a) (b)

Figure 5.6: (a) Inlet monomer flowrate (Q), and (b) Jacket cooling water flowrate (Q_w) for the living chain styrene polymerization reactor. Fault occurs at 5 min and is rectified at 75 min. Dashed lines (- -) show the input profile when the controller tries to maintain nominal operation despite fault in inlet concentration stream and the solid lines (—) show the input profile for the case when the safe-parking framework is implemented.

5.4 is utilized to select the operating point during fault rectification. Some of the candidate safe-park points, deemed acceptable from a steady state stand point and a stability region standpoint (verified via presence in the easy to compute Π^+ set instead of the Ω^+ set, albeit relying on successive feasibility of the control law) are shown in Table 5.4. From the set of candidate safe-park points, a safe-park point which produces styrene with quality closest to the desired values is chosen as a safe-park point. In particular, as $x_{sf,3}$ has polymer quality closest to the desired value, it is chosen as the safe-park point for operating the reactor during fault rectification. The values of the process states corresponding to the safe-park point $x_{sf,3}$ are given in Table 5.5. As shown by the solid lines in Fig. 5.5, the process is stabilized at the safe-park point x_{sf} during fault rectification and nominal operation is resumed after the fault is rectified. The corresponding input profile is shown by dashed lines in Fig. 5.6. The product during the operation at the safe-park point has a number average molecular weight (M_n) of 21,349 gm/mol and polydispersity of 2.72; both of these properties are very close to the desired product qualities. In summary, a fault that precludes continued process operation at the nominal equilibrium point is handled via a safe-parking framework that enables both stable process operation and acceptable product quality during fault rectification, and smooth resumption of nominal operation upon fault rectification.

5.5 Conclusions

In this chapter, we focused on fault tolerant control of living nitroxide-mediated radical polymerization of styrene in a CSTR. First, a model predictive controller was designed and implemented to operate the reactor at an optimal, unstable operating

point. Next, faults were considered that do not allow continuation of nominal operation. A safe-parking framework was designed and shown (via closed-loop simulations) achieve a product during fault rectification that complies with required product specifications, and enable smooth resumption of nominal operation.

Bibliography

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, 2008a.

A. Armaou and M. A. Demetriou. Redesign-free fault-tolerant control systems for a class of reaction-diffusion systems. In *Proc. of the 18th International Symposium on Mathematical Theory of Networks and Systems*, 2008b.

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

Jose Bonilla, Enrique Saldivar, Antonio Flores-Tlacuahuac, Eduardo Vivaldo-Lima, Rudolf Pfaendner, and Fernando Tiscareno-Lechuga. Detailed modeling, simulation, and parameter estimation of nitroxide mediated living free radical polymerization of styrene. *Polymer Reaction Engineering*, 10:227 – 263, 2002.

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.

M.A. Demetriou, K. Ito, and R. C. Smith. Adaptive monitoring and accommodation

of nonlinear actuator faults in positive real infinite dimensional systems. *IEEE Trans. Automat. Contr.*, 52(12):2332 – 2338, 2007.

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

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

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

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

S. Ghantasala and N. H. El-Farra. Robust diagnosis and fault-tolerant control of distributed processes over communication networks, in press. *Int. J. Adapt. Contr. & Sig. Proc.*, 23:699–721, 2008.

N. Huynh and N. Kazantzis. Parametric optimization of digitally controlled nonlinear reactor dynamics using zubov-like functional equations. *J. Math. Chem.*, 38:499–519, 2005.

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

I. Karafyllis and C C. Kravaris. Robust output feedback stabilization and nonlinear observer design. *Syst. & Contr. Lett.*, 54:925–938, 2005.

Roberto Lemoine-Nava, Antonio Flores-Tlachuahuac, and Enrique Saldivar-Guerra. Non-linear bifurcation analysis of the living nitroxide-mediated radical polymerization of styrene in a cstr. *Chem. Eng. Sci.*, 61:370–387, 2006.

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

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

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.

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.

P. Mhaskar. Robust model predictive control design for fault-tolerant control of process systems. *Ind. & Eng. Chem. Res.*, 45:8565–8574, 2006.

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.

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.*, 55:650–659, 2006a.

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, 2006b.

P. Mhaskar, A. Gani, C. McFall, P. D. Christofides, and James F. Davis. Fault-tolerant control of nonlinear process systems subject to sensor faults. *AIChE J.*, 53:654–668, 2007.

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.

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

C. Panjapornpon and M. Soroush. Shortest-prediction-horizon non-linear model-predictive control with guaranteed asymptotic stability. *Int. J. Contr.*, 80:1533–1543, 2007.

Dominick V. Rosato, Nick R. Schott, and Marlene G. Rosator. *Plastics Engineering, Manufacturing & Data Handbook: Plastics Engineering, Manufacturing & Data Handbook.* Springer, 2001.

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

Juan Carlos Verazaluce-Garcia, Antonio Flores-Tlacuahuac, and Enrique Saldivar-Guerra. Steady-state nonlinear bifurcation analysis of a high-impact polystyrene continuous stirred tank reactor. *Ind. & Eng. Chem. Res.*, 39:1972 – 1979, 2000.

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.

Blank Page

Chapter 6

Conclusions and Future Work

6.1 Conclusions

This work considered the problem of control of nonlinear process systems subject to input constraints and faults in the control actuators. A safe-parking framework was developed for handling faults that preclude the possibility of continued operating at the nominal equilibrium point. First, Lyapunov-based model predictive controllers, that allow for an explicit characterization of the stability region subject to constraints on the manipulated input, were designed. The stability region was utilized in selecting 'safe-park' points from the safe-park candidates (equilibrium points subject to failed actuators). Specifically, a candidate parking point was termed a safe-park point if 1) the process state at the time of failure resides in the stability region of the safe-park candidate (subject to depleted control action), and 2) the safe-park candidate resides within the stability region of the nominal control configuration. Performance considerations, such as ease of transition from and to the safe-park point and cost of running the process at the safe-park point, were then quantified and utilized in

choosing the optimal safe-park point. The proposed framework was illustrated using a chemical reactor example and its robustness with respect to parametric uncertainty and disturbances was demonstrated via a styrene polymerization process.

Next, we extended the safe-parking framework to handle practical issues such as model-plant mismatch, disturbances and unavailability of all process state measurements. We proposed robust model predictive controller to handle process parameter uncertainties, disturbances and measurement noise. 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.

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

We then demonstrated the efficacy of proposed safe-parking framework on practical and bigger system. We implemented safe-parking framework for fault tolerant control of living nitroxide-mediated radical polymerization of styrene in a CSTR. First, a model predictive controller was designed and implemented to operate the reactor at an optimal, unstable operating point. Next, faults were considered that do not allow continuation of nominal operation. A safe-parking framework was designed and shown (via closed-loop simulations) achieve a product during fault rectification that complies with required product specifications, and enable smooth resumption of nominal operation.

6.2 Recommendations for Future Work

Recommendations for future work are presented below.

1. The present work considered actuator faults and process equipments faults. Another important class of failure is sensor failures leading to measurement losses. The loss of sensor measurements can render some of process states unobservable and if these unobservable states are unstable, to ensure safety of entire process, it becomes essential that observable process states (or some of the observable process states) be driven to another operating point such that the unstable unobservable process states becomes bounded or stable.

2. In the present work a grid search is used to estimate the stability region and available equilibrium points in failure scenario. The computation requirement for grid search technique increases exponentially with increase in the number of process states. Further work is recommended for using optimization based

approach to estimate the stability region. Here the objective is to find biggest ellipsoid (level set of Lyapunov function) such that the Lyapunov function can be made to decrease for all points inside the ellipsoid. This gives rise to mixed integer nonlinear optimization problem (due to switched control law), which are difficult to solve for global optimal solution. Also, optimization based approaches can be used to select optimal safe-park point. This requires solving optimization problem to find the equilibrium point for the process in failure scenario, such that choosing this equilibrium point as 'safe-park' point will minimize the cost of operation during safe-parking procedure and also will satisfy the stability requirements of 'safe-park' point. If both above problems can be solved as separate optimization problems, next stage can be to combine these two problems to one optimization problem that will, at once, 1) estimate stability regions and 2) find optimal 'safe-park point'.

3. As mentioned in Remark 4.6, the proposed safe-parking framework for plant-wide fault tolerant control can be extended to deal with multi-unit processes with recycle streams. In cases where the effect of the safe-parking of the faulty unit can be absorbed in downstream units, this extension is straight forward as presented in Chapter 4. On the other hand, if the disturbance caused by safe-parking of faulty unit can't be rejected in the downstream units, it becomes necessary to safe-park multiple units simultaneously. Due to presence of recycle stream, the safe-park points for the units can't be determined sequentially, but the safe-park points for all the units must be selected in coordination. This can be accomplished by using overall plant model to calculate the candidate safe-park points for each unit that needs to be safe-parked and then verifying

whether the candidate safe-park point satisfies safe-parking requirements or not. Further work is recommended to explore details of safe-parking for systems with recycled streams.