UCLA
UCLA Electronic Theses and Dissertations

Title
Safe Model Predictive Control Formulations Ensuring Process Operational Safety

Permalink
https://escholarship.org/uc/item/5dr6x4r7

Author
Albalawi, Fahad Ali

Publication Date
2017

Peer reviewed|Thesis/dissertation

eScholarship.org Powered by the California Digital Library
University of California

UNIVERSITY OF CALIFORNIA

Los Angeles

Safe Model Predictive Control Formulations Ensuring Process Operational Safety

A dissertation submitted in partial satisfaction of the

requirements for the degree Doctor of Philosophy

in Electrical Engineering

by

Fahad Ali A Albalawi

2017

ABSTRACT OF THE DISSERTATION

Safe Model Predictive Control Formulations Ensuring Process Operational Safety

by

Fahad Ali A Albalawi

Doctor of Philosophy in Electrical Engineering

University of California, Los Angeles, 2017

Professor Panagiotis D. Christofides, Chair

Model predictive control (MPC) is an advanced control strategy widely used in the process industries and beyond. Therefore, industry is interested in the development of MPC formulations that can enhance safety, reliability, and economic profitability of chemical processes. Motivated by these considerations, this dissertation focuses on the development of methods for integrating process operational safety and process economics within model predictive control system designs. To accomplish these critical control objectives, various economic model predictive control (EMPC) schemes that maintain the process state within a safety region in state-space while optimizing process economics are considered for the first time. The safety region is assumed in the first part of the dissertation to be a level set of a Lyapunov function which is made forward invariant through appropriate MPC design. However, safety-based constraints may define a safety region that is irregularly shaped, and therefore, the safety region may not be taken to be a level set of a Lyapunov function in general. Hence, the second part of this thesis proposes an economic model predictive control (EMPC) formulation that utilizes a Safeness Index function (a function that measures the safeness of points in state-space) as a hard constraint to define a safe region of operation termed the safety zone. Such a safety zone is not restricted to be a level set of a Lyapunov function and may be irregularly shaped. While the two initial safety-based EMPC formulations explicitly

handle process safety and economic considerations, they are centralized in nature and may lead to control action calculations that exceed the allowable sampling period. To address this potential practical limitation of the centralized safety-based EMPC designs, the third part of this dissertation addresses the development of distributed EMPC architectures with safety-based constraints. Both sequential and iterative distributed control architectures, and the partitioning of inputs between the various optimization problems in the distributed structure based on their impact on process operational safety, are investigated. Chemical process examples will be used throughout the thesis to demonstrate the applicability and effectiveness of the proposed control methods.

The dissertation of Fahad Ali A Albalawi is approved.

Jason Speyer

Dante A. Simonetti

Samuel Coogan

Panagiotis D. Christofides, Committee Chair

University of California, Los Angeles

2017

Contents

List of Figures

ACKNOWLEDGEMENTS

I would first like to thank my advisor, Professor Panagiotis D. Christofides, for his great support throughout my doctoral work. I feel very blessed that I have accomplished my Ph.D. under his supervision during my time at UCLA. Professor Panagiotis D. Christofides has been supportive and has given me the freedom to pursue various projects. He has also provided insightful discussions about the research. I would like to thank Professor Jason Speyer, Professor Dante Simonetti, and Professor Sam Coogan for agreeing to serve on my doctoral committee.

I would like to thank Helen Durand for being an excellent colleague who worked closely with me on all of our group projects. Our teamwork combined our strengths, thereby accelerating our research progress. Furthermore, I would like to thank Andres Aguirre, Anh Tran, Marquis Crose, Zhe Wu and Zhihao Zhang, Mathew Ellis, Liangfeng Lao and Anas Alanqar for being excellent and helpful colleagues. Also, a special thanks, in particular, to Anh Tran and Zhe Wu for their comments in proofreading my dissertation. I would like to thank all of my lab mates during my graduate career.

I am grateful for the love, encouragement, and tolerance of Daniya Aljasir , the woman who has made all the difference in my life. Without her patience and sacrifice, I could not have completed this thesis. A special word of thanks also goes to my brothers Mohammed and Yasser Albalawi and my sisters Saleha and Norah Albalawi for their continuous support and encouragement.

I would like to dedicate this thesis to my father, Ali Albalawi, and my mother, Fatima Albadi. I am so grateful for all the moral support and the amazing chances they've given me over the years.

Finally, I would like to thank my grandmother Norah Albadi. I have been extremely fortunate in my life to have a grandmother who has shown me unconditional love and support. The relationships and bonds that I have with my grandmother hold an enormous amount of meaning to me. I admire her for all of her accomplishments in life, for her independence, for her hierarchical role in our family, and for all of the knowledge and wisdom that she has passed on to her grandchildren over the years. Personally, my grandmother has played an important role in the development of my identity and shaping the individual that I am today. She has taught me a great deal about the aging

process and about growing old gracefully.

Financial support from the Department of Energy (DOE), the National Science Foundation (NSF) and Taif University is gratefully acknowledged, and my work could not have been done without this support.

Chapter 2 is a version of: F. Albalawi, A. Alanqar, H. Durand, and P. D. Christofides. A Feedback control framework for safe and economically-optimal operation of nonlinear processes. *AIChE J.*, 62:2391-2409, 2016.

F. Albalawi, A. Alanqar, H. Durand, and P. D. Christofides. Simultaneous control of safety constraint sets and process economics using economic model predictive control. *American Control Conference (ACC)*, 2016, 5062–5067.

Chapter 3 is a version of: F. Albalawi, H. Durand, A. Alanqar and P. D. Christofides. Achieving operational process safety via model predictive control. *Journal of Loss Prevention in the Process Industries*, in press, 2017.

F. Albalawi, H. Durand and P. D. Christofides. Operational safety of chemical processes via safe model predictive control. *Proceedings of Foundations of Computer Aided Process Operations / Chemical Process Control*, Tucson, Arizona, 2017.

Chapter 4 is a version of: F. Albalawi, H. Durand and P. D. Christofides. Distributed economic model predictive control for operational safety of nonlinear processes. *AIChE J.*, in press, 2017.

Chapter 5 is a version of: F. Albalawi, H. Durand and P. D. Christofides. Process operational safety using model predictive control based on a process Safeness Index. *Computers & Chemical Engineering*, 104:76-88, 2017.

F. Albalawi, H. Durand, A. Alanqar and P. D. Christofides. Process safeness index: its definition and use in economic model predictive control to ensure process operational safety. *American Control Conference (ACC)*, Seattle, Washington, in press, 2017.

Chapter 6 is a version of: F. Albalawi, H. Durand and P. D. Christofides. Distributed economic model predictive control with safeness-index based constraints for nonlinear systems. *System & Control Letters*, submitted, 2017.

VITA

2003–2008	Bachelor of Science, Electrical Engineering Department of Electrical Engineering Umm Alqura University
2011–2013	Master of Science, Electrical Engineering Department of Electrical and Computer Engineering George Washington University
2013	Graduation Distinction George Washington University
2013–2017	Graduate Student Researcher / Teaching Assistant Department of Electrical Engineering University of California, Los Angeles

PUBLICATIONS

1. F. Albalawi, H. Durand, A. Alanqar and P. D. Christofides, "Achieving operational process safety via model predictive control," *Journal of Loss Prevention in the Process Industries*, in press.

2. F. Albalawi, A. Alanqar, H. Durand and P. D. Christofides, "A feedback control framework for safe and economically-optimal operation of nonlinear processes," *AIChE Journal*, 62, 2391-2409, 2016.

3. F. Albalawi, H. Durand and P. D. Christofides, " Distributed economic model predictive control for operation safety of nonlinear processes," *AIChE Journal*, in press.

4. F. Albalawi, H. Durand and P. D. Christofides, " Process operational safety using model predictive control based on a proses Safeness Index," *Computers & Chemical Engineering*, 104, 76-88, 2017.

5. F. Albalawi, H. Durand and P. D. Christofides, " Distributed economic model predictive control with Safeness-Index based constraints," *Systems & Control Letters*, submitted.

6. F. Albalawi, H. Durand and P. D. Christofides, " Process operational safety via model predictive control: recent results and future research directions," *Computers & Chemical Engineering*, submitted.

7. F. Albalawi, H. Durand, A. Alanqar and P. D. Christofides, "Process Safeness Index: its definition and use in economic model predictive control to ensure process operational safety," *Proceedings of the American Control Conference*, in press, Seattle, Washington, 2017.

8. F. Albalawi, H. Durand and P. D. Christofides, "Operational safety of chemical processes via safe model predictive control," *Proceedings of the International Conference on Chemical Process Control*, Tucson, Arizona, 2017.

9. F. Albalawi, A. Alanqar, H. Durand and P. D. Christofides, "Simultaneous control of safety constraint sets and process economics using economic model predictive control," *Proceedings of the American Control Conference*, 5062-5067, Boston, Massachusetts, 2016.

10. F. Albalawi, H. Durand, A. Alanqar and P. D. Christofides, "Integrating process safety consideration in Lyapunov-based model predictive control," *Proceedings of IFAC 2017 World Congress*, in press, Toulouse, France, 2017.

11. F. Albalawi, H. Durand and P. D. Christofides, "Distributed economic MPC with safety-based constraints for nonlinear systems," *Proceedings of IFAC 2017 World Congress*, in press, Toulouse, France, 2017.

12. A. Alanqar, H. Durand, F. Albalawi and P. D. Christofides, "An economic model predictive control approach to integrated production management and process operation," *AIChE Journal*, 63, 1892-1906, 2017.

13. A. Alanqar, H. Durand, F. Albalawi and P. D. Christofides, "Integrating production scheduling and process operation via economic model predictive control," *Proceedings of the 55th IEEE Conference on Decision and Control*, 3190-3195, Las Vegas, Nevada, 2016.

Chapter 1

Introduction

1.1 Economic Model Predictive Control

Model predictive control (MPC) is an optimization-based control strategy that can optimally control multiple-input multiple-output nonlinear systems by solving an on-line optimization problem subject to input and state constraints. The conventional formulations of MPC use a quadratic performance index along a finite prediction horizon to steer the system to the optimal (economically) steady-state. While this strategy (steady-state optimization and operation) has been traditionally used in chemical process industries, steady-state operation may not necessarily be the economically best operation strategy especially considering the volatility of economic considerations. Recently, economic model predictive control (EMPC) has been introduced as an alternative approach to the traditional approach to economic process optimization and control.[15, 18, 36, 41, 45, 46, 70, 82] Using an (non-quadratic) objective function that directly reflects the process economics, EMPC may operate a system in a potentially time-varying fashion to optimize the process economics, beyond what can be achieved with steady-state operation. Unlike traditional control techniques, EMPC is able to maximize operating profit through adapting process operating conditions in real-time to account for feedstock variability, feedstock availability, or product demand and/or to minimize operating cost through real-time energy management and accounting for raw material prices since EMPC

accounts directly for the process economics.

Due to the flexibility and profitability of the EMPC, many recent research works have integrated EMPC with different control objectives including: incorporating Lyapunov-based constraints into EMPC to achieve two switching operation modes,[43] incorporating production management into EMPC,[4,5] proof of asymptotic stability of EMPC formulated without terminal constraints,[41] proposition of an EMPC scheme with a self-tuning terminal cost,[70] and asymptotic average performance bounds for EMPC using a generalized terminal region constraint[71] (see, also, the review[37] for more recent results on EMPC).

1.2 Process Operational Safety in the Chemical Process Industries

The environmental damage and loss of life caused by catastrophic accidents in the chemical process industries motivate the development of new methods that can improve operational safety of chemical plants. The two traditional methods for protecting against unsafe scenarios in these industries are improving process inherent safety (i.e., the innate safeness of the process based on its chemistry and physics) and designing effective control systems.[32] Despite the protection and operation procedures that these methods offer to keep running chemical plants safely, catastrophic incidents and disasters continue to happen causing human loss and environmental damages.[2,3] Since it is not possible to eliminate all hazards at a plant, a safety system, comprised of several independent layers, should be added (Figure 1.1). Ideally, the layers of the safety system should not be activated regularly because a basic process control system (BPCS) regulates process variables to their set-points. When the BPCS fails to keep the process variables within acceptable ranges due to, for example, equipment faults or unusually large process disturbances, alarms are triggered that alert operators so that actions can be taken to prevent further unsafe deviations. If the process variables subsequently further exceed allowable values, the emergency shutdown system (ESS) is triggered, which takes automatic and extreme actions such as forcing a valve to its fully open position to

bring the process to a safer state of operation. Safety relief devices such as relief valves are used on vessels that can become highly pressurized quickly, such that the control system, alarms, and ESS alone may not prevent an explosion. Over the past decades, many research works have been conducted to analyze the root causes of why the safety system (Figure 1.1) used in industry failed to prevent these accidents.[51,52] The consistency of these accidents throughout chemical process plant history[61] has led some researchers to observe that the philosophy used in the design of the control and safety system layers (i.e., designing barriers against specific unsafe scenarios using the safety system) is quite limited, particularly as economic considerations drive more optimized and integrated system designs,[40,42,60,74] and that a systems approach to analyzing process safety should instead be used. One step toward this systems approach is by incorporating safety considerations within the BPCS. The single-input/single-output controllers traditionally used within the BPCS cannot account for factors that are important to process safety such as multivariable interactions and state/input constraints. Alternatively, advanced model-based control methodologies that utilize constrained optimization such as model predictive control (MPC) can account for these factors and thus can be integrated with safety considerations.[58,64,66,80] A large number of works in the MPC literature (including works related to economic MPC (EMPC)[15,16,33,37,65,76,82,95] which is an important emerging MPC formulation with a non-quadratic objective function) have addressed the robustness and closed-loop stability of MPC (e.g.,[18,24,37,43,44,64,68] and the references therein); however, standard control analysis tools that can be used to establish such properties (e.g., regions of attraction, feasible regions, and conservative state constraints to account for disturbances/uncertainty) do not account for safe process operation.

For example, regions where feasibility and closed-loop stability of a controller are ensured based on mathematical analysis of first-principles models may include regions where certain states exceed allowable ranges (e.g., the temperature or pressure may damage the process equipment). Safety in the sense of fault/abnormality diagnosis and monitoring has been addressed (e.g.,,[89,94 31,38]), as well as integrating fault-tolerance within process control.[13,20,48,54,67,79,92] However, these methods do not address system-wide safety considerations in control for non-faulty oper-

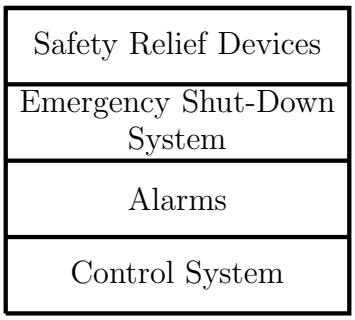

Figure 1.1: Control/safety system layers.[62]

ation. Furthermore, the integration of control and safety systems through a system-wide safety metric (while operating the systems independently) has not been performed, though this has the potential to significantly reduce unnecessary triggering of the safety system and to help in the design of triggers and appropriate actions for automated elements of the ESS and relief systems. This can be particularly beneficial for mitigating alarm overloading,[22,23,39,91] which is the triggering of too many alarms at once, either because of poor alarm design creating frequent alarms that require no operator actions, or too many correct alarms sounding at once triggered by the same root cause. The number of alarms that sound at a chemical process plant each day can be over seven times the recommended number,[34,83] making it difficult for operators to adequately address the alarms, which can lead to environment and plant damage, danger to lives,[85] and reduced operator confidence in the alarm system.[91] Industry[83] and academia[14,19,21,25,69,73,75,93] have addressed alarm issues with techniques based on, for example, models, statistical analysis, and metrics.[1] However, none of these methods integrates safety considerations within the control system to prevent the closed-loop system from reaching conditions where the alarms need to be activated. A broad conclusion of the above literature review is that a systematic methodology for constructing the form of an index that can incorporate control and safety system considerations to aid in improving these system designs while keeping them independent, and designing control systems with provable closed-loop stability and feasibility properties for nonlinear systems and including such an index remain open areas of research.

To tackle this process safety objective, one needs to account for process operational safety

explicitly within the process control design layer (i.e., BPCS), and this only can be done using advanced control techniques such as MPC. Specifically, to enhance both safety and economic tasks of chemical processes in real-time, it is necessary to design a control system that can simultaneously compute safe and economically optimal control actions for nonlinear processes and maintain process closed-loop stability even in the presence of uncertainty. Given all of the above requirements and objectives, EMPC is one natural control methodology to accomplish these tasks. This thesis focuses on incorporating explicit safety-based constraints and Lyapunov-based constraints into EMPC to guarantee process operational safety, in accordance with recent calls for moving into this direction.[37,58]

1.3 Centralized versus Distributed Model Predictive Control for Process Operational Safety

Motivated by a systems-based, control-inspired approach to thinking about safety where a relationship exists between safety and model-based control,[58] an EMPC design that includes explicit constraints on process safety was first proposed in[6] (a description of this scheme will be given in a later chapter). The proposed safety-based controller reduces the region of process operation when required to a smaller region (safety region) when process monitoring logic (referred to as a safety logic unit) indicates that certain regions of state-space away from the steady-state may lead to process safety concerns due to process disturbances. The safety-based controller design was developed with a centralized model predictive control (MPC) structure. For a relatively small process (e.g., one unit), the centralized safety-based EMPC formulation in[6] may be capable of computing an optimal solution that meets the safety-based constraints within a reasonable time frame. However, for large-scale nonlinear process systems, which are the common case in industry, the computational burden of solving a centralized EMPC design with potentially tens or hundreds of optimization variables increases. Therefore, computation time limitations within a sampling period when solving these large-scale nonlinear process systems may reduce the effec-

tiveness of such a controller design for promoting process safety. In addition, the proposed control design in[6] cannot coordinate the control system with the safety system to ensure that both systems account for the limitations of the other, and it also cannot apprise the safety system of the impacts of multivariable interactions on process safety.

To coordinate the control and the safety systems while maintaining their independence for redundancy purposes, a metric termed the Safeness Index that indicates the relative safeness of the process state in state-space (and therefore accounts for interactions between states) was developed in[11] (a description of this framework will be given in a later chapter). The safety system, as well as the control system, can incorporate triggers based on this index by setting thresholds on the value of this index. Similar to the control architecture proposed in,[6] a centralized Lyapunov-based EMPC (LEMPC) scheme with constraints related to thresholds on the Safeness Index was developed in.[11] For many industrial processes (e.g., large-scale nonlinear process systems with tens or hundreds of inputs to be determined by an optimization-based controller like EMPC), the computation time of the centralized design may be significant compared to the length of a sampling period, which reduces the effectiveness of the centralized design for enhancing process safety for such processes. In addition, the safety region is not necessarily an invariant set under the Safeness Index-based MPC design proposed in;[11] as a result, frequent re-optimization (for frequent feedback) may be beneficial for detecting that the closed-loop state has exited the safety zone during a sampling period to cause the controller to drive it back into the safety zone. This computation time issue cannot be handled with decentralized control designs (i.e., multiple controllers utilize the same process model to compute subsets of the entire set of available control actions but without communication between the controllers), because such designs may pose safety concerns since the controllers do not coordinate their actions.[56]

An alternative EMPC architecture that is intended to improve the computation time of the centralized EMPC algorithm is a distributed economic model predictive control (DEMPC) architecture.[28,84,88] Distributed EMPC is a control paradigm in which subsets of the entire set of available control actions are computed by controllers that utilize the same process model, but which com-

municate.[28,88] This EMPC architecture has been investigated for computation time benefits since it can reduce the number of decision variables in each of the distributed optimization problems and may be able to terminate the optimization problems before the optimal solution is found while maintaining feasibility and closed-loop stability of the controller.[26] Distributed designs also can be beneficial from the perspective of fault-tolerance,[28] which is another safety consideration.

A recent research work developed two different DEMPC schemes that reduce the computation time of a centralized EMPC scheme while maintaining similar closed-loop performance.[17] Nevertheless, these two control schemes lack the ability to drive the state of the closed-loop system to a safe region of operation because their formulations do not include safety-based constraints. In addition, the partitioning of inputs between distributed EMPC controllers based on safety considerations and the conditions in which closed-loop stability and recursive feasibility of a nonlinear process are guaranteed under a distributed Safeness Index-based EMPC design and distributed safety-based LEMPC design have not been considered. To date, no work on incorporating safety-based constraints within a distributed economic model predictive controller has been completed.

1.4 Dissertation Objectives and Structure

Motivated by the above considerations, this dissertation focuses on the development of methods for integrating process operational safety and process economics with EMPC design. Various LEMPC formulations that can guarantee process operational safety while also dictating an economically optimal dynamic operating policy and maintaining closed-loop stability and recursive feasibility are proposed. In addition, this work includes a Safeness Index-based LEMPC that can indicate the relative safeness of the process state in state-space (and therefore accounts for interactions between states). To overcome the computation time burden associated with the centralized safety-based LEMPC designs, various distributed safety-based LEMPC paradigms that can have less computation time than the centralized safety-based LEMPC are developed. The dissertation has the following structure:

Chapter 2 presents three safety-based LEMPC schemes that can combine feedback control, process economics and safety considerations. The first scheme utilizes a contractive constraint to compute control actions that can drive the closed-loop state to a safe region of operation at least as quickly as a stabilizing Lyapunov-based controller would in a worst case while the second scheme utilizes a sufficiently long prediction horizon and a region constraint to ensure that the state is within the safety region by a specific time. The third scheme includes two EMPC formulations where the first one incorporates a slack variable to achieve a smooth transition between the regular region of operation and the safety region. The second formulation dynamically controls the upper bound on the Lyapunov function directly. For a sufficiently small sampling period, recursive feasibility and closed-loop stability of a class of nonlinear systems under the safety-LEMPC schemes for nominal operation and in the presence of uncertainty are rigorously analyzed.

For the specific case in which the EMPC objective function is quadratic, chapter 3 presents two LMPC designs with safety-based constraints that can integrate feedback control and process operational (functional) safety within a unified framework. The motivation for the proposed safety-LMPC designs is to drive the closed-loop state to a safe region of operation at a desired rate, which cannot easily be accomplished by tuning the weighting matrices in the quadratic objective function. The safety-LMPC's vary the upper bound on the level set of the Lyapunov function to achieve the improved rate of approach to the safety region, and they can also be modified to shift the region of operation from a level set around one steady-state to a level set around another. For a sufficiently small sampling period, a proof of recursive feasibility and closed-loop stability of a class of nonlinear systems under one of the safety-LMPC formulations in the presence of uncertainty is given.

Chapter 4 develops two distributed (sequential and iterative) Safety-DLEMPC schemes that may have significantly less on-line computation time than the centralized safety-based LEMPC while achieving similar closed-loop performance and safety constraints satisfaction. An implementation strategy and mathematical formulation for the Safety-Sequential-DLEMPC design and the Safety-Iterative-DLEMPC design are developed. For a sufficiently small sampling period,

proofs of recursive feasibility and closed-loop stability of a class of nonlinear systems under the Safety-S-DLEMPC and Safety-I-DLEMPC formulations in the presence of uncertainty are given. A catalytic reactor example is utilized to illustrate the computation time advantages of the proposed iterative and sequential Safety-DLEMPC strategies with respect to the centralized Safety-LEMPC.

Chapter 5 develops a Safeness Index-based LEMPC paradigm that can coordinate, for the first time, the control and safety systems within a chemical process plant. Specifically, an approach for defining the functional form of the Safeness Index is presented, and a methodology of choosing the threshold of the Safeness Index is given. To demonstrate the use of this Safeness Index within a control system, an LEMPC scheme with a hard Safeness Index-based constraint is presented to integrate feedback control, process safety and process economics within a unified framework. An implementation strategy is developed that is guaranteed, under sufficient conditions, to drive the closed-loop state into the region where the Safeness Index is less than a desired threshold when initiated from any state within the stability region.

Chapter 6 develops sequential and iterative distributed economic model predictive control (DEMPC) architectures with constraints based on the Safeness Index. The DEMPC's may have lower computation time than a centralized economic model predictive control (EMPC) design with Safeness Index-based constraints, without significantly limiting closed-loop economic performance, which enhances their practicality and ability to improve process operational safety. Sufficient conditions are derived under which the implementation strategies for the DEMPC's guarantee closed-loop stability.

Finally, Chapter 7 summarizes the contributions of this dissertation.

Chapter 2

A Feedback Control Framework for Safe and Economically-Optimal Operation of Nonlinear Processes

2.1 Introduction

This chapter addresses the task of developing three EMPC schemes that adjust in real-time the size of the safety sets in which the process state should reside in order to ensure safe process operation and feedback control of the process state while optimizing economics via time-varying process operation. Recursive feasibility and closed-loop stability are established for a sufficiently small EMPC sampling period. The proposed schemes, which effectively integrate feedback control, process economics and safety considerations, are demonstrated with a chemical process example. The results of this chapter originally appeared in.[6,7]

2.2 Preliminaries

2.2.1 Notation

In this chapter, $t_k = k\Delta$, $k = 0, 1, 2, ...$ refers to synchronous time instants separated by a sampling period Δ. The Euclidean norm of a vector is denoted by $|\cdot|$. A function $\alpha : [0, a) \to [0, \infty)$ with $\alpha(0) = 0$ belongs to class $\mathscr{K}$ if it is continuous and strictly increasing. A level set of a scalar-valued positive definite function $V(x)$ is defined to be the set $\Omega_\rho := \{x \in R^n \mid V(x) \leq \rho\}$. Set subtraction is denoted using '/' (i.e., $x \in A/B := \{x \in R^n \mid x \in A,\ x \notin B\}$). The notation $diag(a_1, ..., a_m)$ signifies a diagonal $m \times m$ matrix with diagonal elements $a_1, ..., a_m$.

2.2.2 Class of Nonlinear Process Systems

The class of nonlinear process systems considered is as follows:

$$\dot{x}(t) = f(x(t), u(t), w(t)) \tag{2.1}$$

where $x(t) \in \mathbb{R}^n$ is the state vector of the system, and $u(t) \in \mathbb{R}^m$ and $w(t) \in \mathbb{R}^l$ are the control (manipulated) input vector and the disturbance vector, respectively. The admissible input values are restricted to m nonempty convex sets $U_i \subseteq \mathbb{R}$, $i = 1, \ldots, m$, where $U_i := \{u_i \in \mathbb{R} : u_i^{\min} \leq u_i \leq u_i^{\max}\}$, and $u_i^{\max}$ and $u_i^{\min}$, $i = 1, \ldots, m$, are the magnitudes of the input constraints which result from the physical constraints on the control actuators. We assume that f is a locally Lipschitz vector function of its arguments and that the state of the system of Eq. 2.1 is synchronously sampled at time instances $t_k = t_0 + k\Delta,\ k = 0, 1, \ldots$, where Δ is the sampling period and t_0 is the initial time. The disturbance $w(t)$ is bounded within the set $W := \{w \in \mathbb{R}^l : |w| \leq \theta, \theta > 0\}$ (i.e., $w(t) \in W$). We assume that the origin is an equilibrium point of the unforced nominal system which implies that $f(0, 0, 0) = 0$.

2.2.3 Lyapunov-Based Controller Assumption

We consider nonlinear systems that are stabilizable in the sense that there exists a Lyapunov-based controller $h(x) = [h_1(x) \cdots h_m(x)]^T$ which renders the origin of Eq. 2.1 with $w(t) \equiv 0$ (the nominal closed-loop system) asymptotically stable with $h_i(x) \in U_i$, $i = 1, \ldots, m$, inside a given stability region Ω_ρ. We further assume the existence[49,63] of a sufficiently smooth Lyapunov function $V(x)$ for the nominal closed-loop system and class $\mathscr{K}$ functions $\alpha_i(\cdot)$, $i = 1,2,3,4$ such that the following inequalities hold:

$$\begin{gathered} \alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|) \\ \frac{\partial V(x)}{\partial x} f(x, h_1(x), \ldots, h_m(x), 0) \leq -\alpha_3(|x|) \\ \left| \frac{\partial V(x)}{\partial x} \right| \leq \alpha_4(|x|) \\ h_i(x) \in U_i,\ i = 1, \ldots, m \end{gathered} \tag{2.2}$$

for all $x \in D \subseteq R^n$ where D is an open neighborhood of the origin. We define a level set of the Lyapunov function within which $\dot{V}$ is negative as the stability region Ω_ρ of the process of Eq. 2.1 under $h(x)$ (where $\Omega_\rho \subseteq D$; see, for example,[27,35,53,59] for results on the design of stabilizing control laws).

When x is maintained within the compact set Ω_ρ, $u_i \in U_i$, $i = 1, ..., m$, and $w \in W$, we have from the continuity of x, the local Lipschitz property of f, and the smoothness of $V(x)$ that there exist positive constants M, L_x, L_w, L_x^* and L_w^* such that the following inequalities hold:

$$|f(x(t), u(t), w(t))| \leq M \tag{2.3}$$

$$|f(x, u, w) - f(x^*, u, 0)| \leq L_x |x - x^*| + L_w |w| \tag{2.4}$$

$$\left| \frac{\partial V(x)}{\partial x} f(x, u, w) - \frac{\partial V(x^*)}{\partial x} f(x^*, u, 0) \right| \leq L_x^* |x - x^*| + L_w^* |w| \tag{2.5}$$

for all $x, x^* \in \Omega_\rho$, $u_i \in U_i$, $i = 1, \ldots, m$, and $w \in W$.

2.2.4 Lyapunov-Based Economic Model Predictive Control (EMPC)

Lyapunov-based economic model predictive control (LEMPC) is an optimization-based control strategy implemented in a receding horizon fashion that utilizes the Lyapunov-based controller $h(x)$ as follows:[43]

$$\min_{u\in S(\Delta)} \quad \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau),u(\tau))\,d\tau \tag{2.6a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t),u(t),0) \tag{2.6b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{2.6c}$$

$$u_i(t) \in U_i,\ i=1,\ldots,m,\ \forall\, t\in[t_k,t_{k+N}) \tag{2.6d}$$

$$V(\tilde{x}(t)) \le \rho_e,\ \forall\, t\in[t_k,t_{k+N})$$

$$\text{if } x(t_k)\in\Omega_{\rho_e} \tag{2.6e}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k),u(t_k),0) \le \frac{\partial V(x(t_k))}{\partial x} f(x(t_k),h(x(t_k)),0)$$

$$\text{if } x(t_k)\notin\Omega_{\rho_e} \tag{2.6f}$$

where the piecewise constant input trajectory $u(t)$ is the decision variable of the optimization problem defined over the prediction horizon with N sampling periods of length Δ, and the predicted state trajectory is denoted by $\tilde{x}(t)$. The nominal model of Eq. 2.1 is used to predict the evolution of the system over the prediction horizon (Eq. 2.6b) where the initial condition of the dynamic system is obtained through a state measurement at the current sampling time t_k (Eq. 2.6c). Eq. 2.6a is the objective function of the LEMPC design, where the stage cost $L_e(\tilde{x},u)$ reflects the process economics of the class of nonlinear systems of Eq. 2.1. The constraint of Eq. 2.6d restricts the control actions $u(t)$ to be within the admissible set over the prediction horizon.

In Mode 1 (Eq. 2.6e), the LEMPC optimizes the economic cost function of Eq. 2.6a in a time-varying fashion when the state measurement of Eq. 2.6c is within the region Ω_{ρ_e}, which is a subset of Ω_ρ. This subset Ω_{ρ_e} is selected to make the stability region Ω_ρ a forward invariant

set for the closed-loop process under LEMPC in the presence of disturbances (i.e., if the process is initialized within Ω_ρ, the closed-loop state is maintained within Ω_ρ for all time). In Mode 2 (Eq. 2.6f), which is activated when $x(t_k) \in \Omega_\rho / \Omega_{\rho_e}$, the contractive constraint utilizes the explicit stabilizing controller $h(x)$ to drive the closed-loop state back into Ω_{ρ_e} by computing control actions that decrease the value of the Lyapunov function at least as much as the decrease given by the stabilizing controller.

2.3 Safety-LEMPC Structure

The major contribution of this dissertation is the development of control schemes that address safety in a control design framework through the incorporation of constraints based on safety considerations. In this chapter, three LEMPC schemes (termed safety-LEMPC schemes) are presented that couple the ability of LEMPC to optimize profit with its ability to handle safety considerations by accounting for multivariable interactions, constraints, and a general objective function. These safety-LEMPC schemes add various safety-based constraints to the standard formulation of LEMPC in Eq. 2.6 so that safety is enforced as a constraint of operation, which allows for economic optimization to be pursued among all solutions to the optimization problem that satisfy the safety criteria.

In this chapter, we provide descriptions of the three proposed safety-LEMPC schemes with safety-based constraints. Specifically, a detailed description of the implementation strategy for the safety-LEMPC schemes, the formulations of the schemes, and a chemical process example for each scheme are presented. Moreover, provable stability and feasibility properties of the safety-LEMPC's are given.

2.3.1 Implementation Strategy

The classical LEMPC design[43] dictates time-varying operation to maximize the profit while maintaining the closed-loop state of the process in the stability region Ω_ρ. The stability region Ω_ρ

may be estimated as the largest level set of the Lyapunov function where the time-derivative of the Lyapunov function is negative along the closed-loop state trajectories of the nominal system of Eq. 2.1 under $h(x)$ for all points in the level set. However, there may be regions in Ω_ρ within which it becomes unsafe to operate the process for some period of time due to disturbances (e.g., significant disturbances in the concentration of the feed stream, disturbances in ambient temperature, actuator problems such as a sticking valve). In such scenarios, it is necessary to change the allowable region of operation in real-time from Ω_ρ to a smaller level set of the Lyapunov function where safe process operation is achieved to maintain the closed-loop state within a safe region of operation. In this chapter, we present three LEMPC schemes with safety-based constraints called safety-LEMPC that can update the level set of the Lyapunov function online to tackle the following two tasks:

Task 1: Driving the closed-loop state of the process of Eq. 2.1 under the safety-LEMPC into a safe region of operation.

Task 2: Maintaining the closed-loop state of the process of Eq. 2.1 under the safety-LEMPC in this safe region of operation.

Figure 2.1 depicts the implementation strategy of the safety-LEMPC paradigm. As shown in Figure 2.1, a safety logic unit determines an appropriate level set for safe process operation by using data on the probability of potential failures of process equipment or software components, measurement feedback of the process state and the estimated future process state trajectory. If it is determined that an equipment or software failure or other unsafe scenario is likely, the safety logic unit communicates the most profitable safety set-point ρ_{sp} to the safety-LEMPC to cause it to drive the closed-loop state to a safe region of operation termed the safety region $\Omega_{\rho_{sp}}$ and maintain the process operation there. The control actions computed by the safety-LEMPC will be applied to the plant in a sample-and-hold fashion, and the measured state will be fed back to both the safety-LEMPC for controller robustness and the safety logic unit so that the safety level set will be re-evaluated if necessary.

Remark 2.1 *If no process faults or unsafe conditions are predicted by the safety logic unit, ρ_{sp} will*

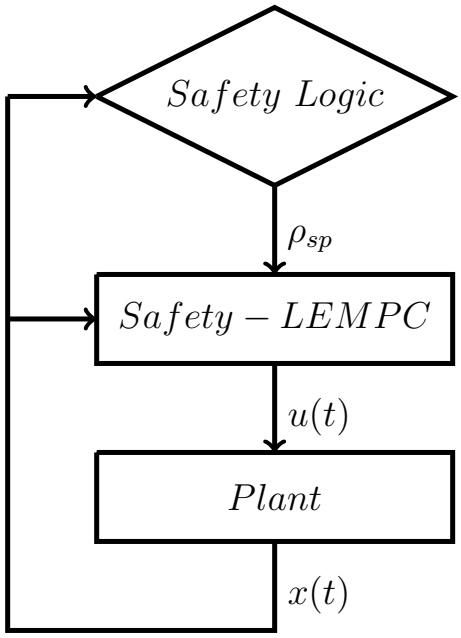

Figure 2.1: The implementation strategy of the safety-LEMPC paradigm

be chosen as the largest level set in the stability region where closed-loop stability in the presence of uncertainty is guaranteed in order to maximize the economic measure of the safety-LEMPC.

Remark 2.2 *In Figure 2.1, the safety logic unit receives the state measurement from the plant regularly; however, the safety logic unit may communicate a new value of ρ_{sp} to the safety-LEMPC less frequently.*

Remark 2.3 *The safety-LEMPC schemes that will be presented are not intended to sacrifice process safety for economic performance. Rather, the three schemes to be presented are intended for different purposes (e.g., one scheme may be better suited for processes where rapid and safety-critical switches of the region of operation are necessary, while another may be better suited for processes where the transition to a new region of operation can be slower without immediate negative consequences, such as a process for which high temperature operation is acceptable for a small period of time though it is safer to move it to a region where the temperature is lower after this time to avoid, for example, material weakening). A control engineer would choose the desired scheme and tune any parameters of the desired scheme in a manner that provides acceptable con-*

trol and safety for a given process. Advantages and disadvantages of the three safety-LEMPC's will be presented in the discussion of each below to elucidate some of the factors that should be considered when selecting a safety-LEMPC scheme. The safety-LEMPC system is not intended to replace traditional process safety systems. It is, however, intended to be used in place of other EMPC schemes that may be used to control a process to augment the traditional safety systems that would also be used to provide an additional means of increasing process safety.

2.4 Scheme 1: LEMPC Using Level-Set Switching

As noted in the "Implementation Strategy" section, the two tasks of the safety-LEMPC are to shift the region of operation to a safer zone and to maintain the closed-loop states within this safer zone. The first considered scheme tackles these tasks by applying the standard LEMPC scheme of Eq. 2.6 (with the Mode 1 and Mode 2 constraints defined with respect to Ω_{ρ_e}) until a switching time t_1 at which time it is desired that the closed-loop state moves toward a lower level set $\Omega_{\rho_{sp}}$ (the safety region) that is within the stability region. At this time, the level set that determines whether the Mode 1 or Mode 2 constraint should be used is re-defined in terms of $\Omega_{\bar{\rho}_{sp}}$, which is a subset of $\Omega_{\rho_{sp}}$ defined to make $\Omega_{\rho_{sp}}$ an invariant set under the safety-LEMPC in the presence of disturbances/uncertainty once the state enters $\Omega_{\rho_{sp}}$ (i.e., the relationship between $\Omega_{\bar{\rho}_{sp}}$ and $\Omega_{\rho_{sp}}$ is similar to that between Ω_{ρ_e} and Ω_ρ). Thus, the effect of this safety-LEMPC scheme is to enforce the Mode 2 contractive constraint starting from the state $x(t_1) \in \Omega_\rho$ until the closed-loop state enters $\Omega_{\bar{\rho}_{sp}}$, so that the rate at which the state approaches the safety region is no worse than the worst-case rate at which the state would approach $\Omega_{\bar{\rho}_{sp}}$ under the Lyapunov-based controller $h(x)$. Due to the closed-loop stability property of the explicit stabilizing controller $h(x)$, this scheme is guaranteed to drive the closed-loop state to the lower level set $\Omega_{\bar{\rho}_{sp}}$ in the presence of uncertainty.[72] Once the state enters $\Omega_{\bar{\rho}_{sp}}$, the safety-LEMPC dictates time-varying operation to maximize the profit while the measured state remains within $\Omega_{\bar{\rho}_{sp}}$, but uses the contractive constraint when $x(t_k) \in \Omega_{\rho_{sp}}/\Omega_{\bar{\rho}_{sp}}$ to ensure process operation is maintained within the safety

region $\Omega_{\rho_{sp}}$ in the presence of disturbances/uncertainty (the proof of this will be clarified in the section "Feasibility and stability analysis").

The formulation of this control strategy is presented in the following optimization problem:

$$\max_{u\in S(\Delta)} \quad \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau),u(\tau))\,d\tau \tag{2.7a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t),u(t),0)$$

$$\tilde{x}(t_k) = x(t_k) \tag{2.7b}$$

$$u_i(t) \in U_i,\ i=1,\ldots,m,\ \forall\, t\in[t_k,t_{k+N}) \tag{2.7c}$$

$$V(\tilde{x}(t)) \le \hat{\rho},\ \forall\, t\in[t_k,t_{k+N}) \tag{2.7d}$$

$$\hat{\rho}=\rho_e, \quad \text{if } x(t_k)\in\Omega_{\rho_e} \text{ and } t_k < t_1$$

$$\hat{\rho}=\bar{\rho}_{sp}, \quad \text{if } x(t_k)\in\Omega_{\bar{\rho}_{sp}} \text{ and } t_k \ge t_1$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k),u(t_k),0) \le \frac{\partial V(x(t_k))}{\partial x} f(x(t_k),h(x(t_k)),0) \tag{2.7e}$$

$$\text{if } x(t_k)\notin\Omega_{\rho_e} \text{ and } t_k < t_1 \text{ or if } x(t_k)\notin\Omega_{\bar{\rho}_{sp}} \text{ and } t_k \ge t_1$$

Remark 2.4 *Although this scheme is guaranteed to drive the closed-loop state of Eq. 2.1 to the desired safety region, it is not guaranteed to do so in a fast or proactive fashion (i.e., there is no adjustable parameter in this scheme that can be changed to modify the time that it takes to drive the closed-loop state into $\Omega_{\rho_{sp}}$ after t_1). Often, safety constraints are required to be satisfied in a measurable amount of time; as a result, this scheme may present an issue for practical implementation in certain scenarios. However, it is also possible to perform extensive closed-loop simulations of the process under $h(x)$ in the presence of bounded disturbances/uncertainty for initial values $x(t_1)\in\Omega_\rho$ throughout the stability region before implementing this safety-LEMPC scheme. From these simulations, it is possible to estimate the worst-case rate of approach to a variety of possible safety level sets to determine whether the rate of transition from Ω_ρ to $\Omega_{\rho_{sp}}$ would be expected to*

be acceptable for a given process.

Remark 2.5 *The economic optimality of a feasible control action plays a significant role in the safety-LEMPC's selection of control actions in this scheme. Because the constraint of Eq. 2.7e only requires that the state move toward $\Omega_{\rho_{sp}}$ at least as quickly as it would under $h(x)$ in a worst case, the LEMPC will choose a control action that maximizes profit during this approach since that is the required objective in this case, and thus it will not choose a different control action that may cause the closed-loop state to more quickly approach the safety region but with less economic benefit during this approach. However, the emphasis of this scheme on economics during the approach to the safety region as opposed to the speed with which the approach to the safety region occurs is an important consideration when determining whether this controller is the best safety-LEMPC to apply for a given process. In circumstances where the known Lyapunov-based controller does not provide a satisfactory worst-case rate of approach of the process state to the safety region, this more economically-focused safety-LEMPC may be inadequate for ensuring that the safety region is approached in the timeframes that may be desired. However, for processes for which the worst-case rate of approach to a safety region under $h(x)$ is considered to be acceptable, the economic focus of the LEMPC during the transition to the safety region (the transition period) may be economically beneficial while still ensuring that all safety requirements are met.*

2.4.1 Scheme 1: Application to A Chemical Process Example

In this section, we demonstrate scheme 1 of the safety-LEMPC using a chemical process example. Because this chemical process example will also be used for the demonstration of the other safety-LEMPC schemes developed in this chapter, we will begin with a general statement of the control problem that will be used in the demonstration of all three schemes, and will then focus on the parameters chosen specifically to demonstrate scheme 1, and the closed-loop results for the process under scheme 1.

The chemical process considered is a well-mixed, non-isothermal continuously stirred tank reactor (CSTR) within which a reactant *A* is transformed to a product *B* through the exothermic, irre-

Table 2.1: Parameter values

$T_0 = 300$	K	$F = 5$	$\frac{m^3}{hr}$
$V = 1.0$	m^3	$E = 5 \times 10^4$	$\frac{kJ}{kmol}$
$k_0 = 8.46 \times 10^6$	$\frac{m^3}{kmol\,hr}$	$\Delta H = -1.15 \times 10^4$	$\frac{kJ}{kmol}$
$C_p = 0.231$	$\frac{kJ}{kgK}$	$R_g = 8.314$	$\frac{kJ}{kmolK}$
$\rho_L = 1000$	$\frac{kg}{m^3}$	$C_{As1} = 1.2$	$\frac{kmol}{m^3}$
$T_{s1} = 438$	K	$C_{As2} = 2$	$\frac{kmol}{m^3}$
$T_{s2} = 400$	K	$C_{A0s} = 4$	$\frac{kmol}{m^3}$
$Q_s = 0$	$\frac{kJ}{hr}$		

versible second-order reaction $A \rightarrow B$.[81] The CSTR is fed with pure A at flowrate F, concentration C_{A0}, and temperature T_0, and it is cooled and heated at heat rate Q by a jacket. The concentration of A (C_A) and temperature T in the reactor are modeled using mass and energy balances with standard modeling assumptions as follows:

$$\frac{dC_A}{dt} = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{R_g T}} C_A^2 \tag{2.8a}$$

$$\frac{dT}{dt} = \frac{F}{V}(T_0 - T) + \frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{R_g T}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{2.8b}$$

where ΔH, k_0, E, and R_g are the enthalpy of reaction, pre-exponential constant, activation energy, and ideal gas constant. The reactor volume V, heat capacity C_p, and fluid density ρ_L within the reactor are assumed constant. The values of these parameters are given in Table 2.1.

The two manipulated inputs of the CSTR are the inlet concentration C_{A0} and the heat input/removal rate Q. These manipulated inputs are bounded as follows: $0.5 \leq C_{A0} \leq 7.5\ kmol/m^3$ and $|Q| \leq 5 \times 10^5\ kJ/hr$.

In the operating region of interest, the process model of Eq. 2.1 has one stable steady-state ($[C_{As1}\ T_{s1}]$=[1.2 $\frac{kmol}{m^3}$ 438 K]) and one unstable steady-state ($[C_{As2}\ T_{s2}]$=[2 $\frac{kmol}{m^3}$ 400 K]) corresponding to the steady-state input $[C_{A0s}\ Q_s]$ given in Table 2.1 (steady-states outside the operating region of interest are not considered). The dynamic model of Eq. 2.8 is a member of the class of nonlinear systems of Eq. 2.1 with $w(t) \equiv 0$, where $x = [C_A - C_{As}\ T - T_s]^T$ is the state vector (C_{As}

= C_{As1} or C_{As2}, and T_s = T_{s1} or T_{s2}) and $u = [C_{A0} - C_{A0s}\ Q - Q_s]^T$ is the input vector. In particular, it is an input-affine nonlinear system with the form:

$$\dot{x}(t) = \tilde{f}(x(t)) + g(x(t))u(t) \tag{2.9}$$

The explicit Euler method with an integration time step of $h_c = 10^{-5}\ hr$ was applied to numerically simulate the dynamic model of Eq. 2.8.

The control objective is to maximize the profit of the CSTR process of Eq. 2.8 while driving the closed-loop state trajectories to a safe region of operation when required by controlling the process using a safety-LEMPC scheme. To maximize the profit, the objective function of the safety-LEMPC optimizes the following stage cost, which represents the production rate of B:

$$L_e(x,u) = k_0 e^{-\frac{E}{RgT}} C_A^2 \tag{2.10}$$

The process and basic design parameters of the safety-LEMPC presented above are now used in the demonstration of scheme 1 (and, as noted, that same problem formulation will be used in the demonstration of the other safety-LEMPC schemes developed in this chapter). In the demonstration of scheme 1 using this chemical process example, the process is operated around the stable steady-state of the CSTR with steady-state input values [C_{A0s} Q_s]=[4 $\frac{kmol}{m^3}$ 0 $\frac{kJ}{hr}$]. In addition, we consider a limitation on the amount of reactant material available over a given operating period $t_p = 1.0\ hr$ (i.e., the amount of reactant material used in each operating period must average to that which would be used under steady-state operation) which is described by the following constraint:

$$\frac{1}{t_p}\int_0^{t_p} u_1(\tau)\, d\tau = 0.0\ kmol/m^3. \tag{2.11}$$

The stabilizing controller designed for use in scheme 1 of the safety-LEMPC is a Lyapunov-based controller of the form $h(x) = [h_1(x)\ h_2(x)]^T$. The inlet concentration is set to its steady-state value in order to meet the material constraint of Eq. 2.11 (i.e., $h_1(x) = 0$). The rate of heat input is

determined by the following Sontag control law:[86]

$$h_2(x) = \begin{cases} -\dfrac{L_{\tilde{f}}V + \sqrt{L_{\tilde{f}}V^2 + L_{g_2}V^4}}{L_{g_2}V}, & \text{if } L_{g_2}V \neq 0 \\ 0, & \text{if } L_{g_2}V = 0 \end{cases} \tag{2.12}$$

where $L_{\tilde{f}}V$ and $L_{g_2}V$ are the Lie derivatives of the Lyapunov function $V(x)$ with respect to the vector fields $\tilde{f}(x)$ and $g_2(x)$ respectively. Extensive closed-loop simulations of the CSTR under the Lyapunov-based controller were performed to determine the stability region of the process under $h(x)$ and the corresponding Lyapunov function. A quadratic Lyapunov function of the form $V(x) = x^T P x$ was chosen with P being the following positive definite matrix:

$$P = \begin{bmatrix} 1060 & 22 \\ 22 & 0.52 \end{bmatrix} \tag{2.13}$$

The stability region was estimated to be the largest level set where the time derivative of the Lyapunov function of the closed-loop system was negative. The stability region of the CSTR under the Lyapunov-based controller, which is used in the Lyapunov-based constraint of Eqs. 2.7d-2.7e, was estimated to be $\rho = 368$ (note that because nominal operation was considered, $\rho_e = \rho$). A sampling period $\Delta = 0.01\ hr$ and an operating period of length $t_f = 1\ hr$ were used to simulate the safety-LEMPC using the interior point solver Ipopt.[90] In addition, for this example, the prediction horizon was chosen to be $N = 10$.

The scheme 1 safety-LEMPC design (Eq. 2.7 with the additional material constraint of Eq. 2.11) was applied to the CSTR, with the process states initialized at the stable steady-state, and the process originally operating in Ω_ρ. After half an hour of operation within Ω_ρ, we assume that the safety logic unit determines that it is necessary to reduce the maximum allowable temperature of operation, so it requests a switch of the region of operation from Ω_ρ to $\Omega_{\rho_{sp}}$ where $\rho_{sp} = 294$ (because nominal operation is considered, $\bar{\rho}_{sp} = \rho_{sp}$). Thus, beginning at $t_1 = 0.5\ hr$, the Mode 2 constraint was applied until the closed-loop state was driven into the safety region $\Omega_{\rho_{sp}}$ by de-

creasing the time derivative of the Lyapunov function by at least as much as the decrease given by the stabilizing control law of Eq. 2.12. Once the state entered $\Omega_{\rho_{sp}}$, the process was dynamically operated within the safety region to maximize the process profit in this safe region of operation.

The state-space trajectories of the CSTR are presented in Figure 2.2 and the state and input trajectories are presented in Figure 2.3. In addition, a plot of the Lyapunov function value of the closed-loop system with respect to time is presented in Figure 2.4. As can be seen, the scheme 1 safety-LEMPC design maximized the profit before t_1 by driving the state from the steady-state to the boundary of Ω_ρ. At t_1, the level set that defines the Mode 1 and Mode 2 constraints was updated online, and scheme 1 was successfully able to drive the closed-loop state from Ω_ρ to $\Omega_{\rho_{sp}}$ in 19 sampling periods and to optimize the profit within $\Omega_{\rho_{sp}}$, subject to the constraints, thereafter. The drop in the Lyapunov function value at the end of the operating period occurs to satisfy the material constraint (Eq. 2.11). Although this safety-LEMPC scheme was able to drive the closed-loop state to the safety region $\Omega_{\rho_{sp}}$ in a finite number of sampling periods, the rate of decrease of the Lyapunov function after t_1 was slow, which may not be desirable for safety-critical processes.

2.5 Scheme 2: LEMPC with A Sufficiently Long Prediction Horizon

As demonstrated by the trajectories of the closed-loop CSTR example under scheme 1, the control actions calculated by scheme 1 are chosen to decrease the Lyapunov function of the closed-loop state but to do so in a manner that optimizes the process economics (rather than optimizing the speed with which the control actions drive the closed-loop state into the safety region), which may cause the time between t_1 and the time at which the state enters $\Omega_{\rho_{sp}}$ to be longer than is practically acceptable. Hence, a scheme that can drive the closed-loop state into $\Omega_{\rho_{sp}}$ by t_1 was developed. This second scheme is an LEMPC design with a sufficiently long prediction horizon, a region constraint,[15] and an estimate of the switching time t_1 to drive the closed-loop state into the safety region by t_1 under certain conditions. One of these conditions is that there are no distur-

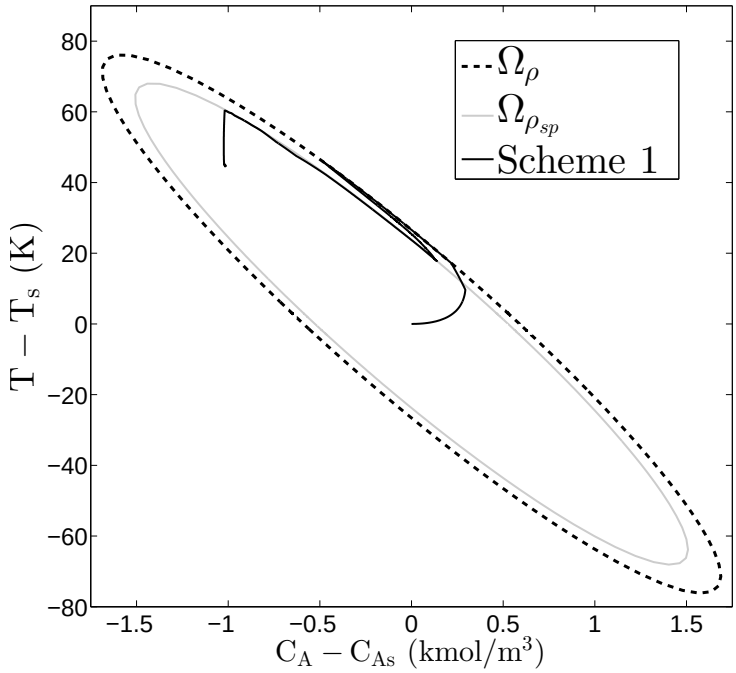

Figure 2.2: The state-space profile for the closed-loop CSTR under the stabilizing safety-LEMPC design of Eq. 2.7 (with Eq. 2.11) for the initial condition $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho = 368$

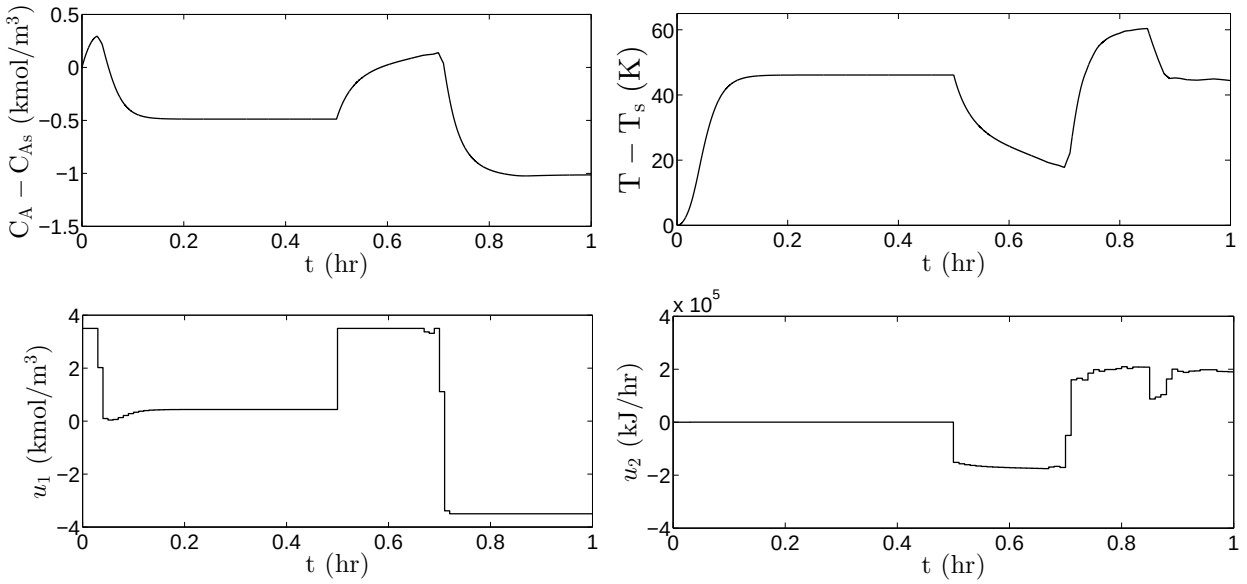

Figure 2.3: Manipulated input and state profiles for the closed-loop CSTR under the stabilizing safety-LEMPC design of Eq. 2.7 (with Eq. 2.11) for the initial condition $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$

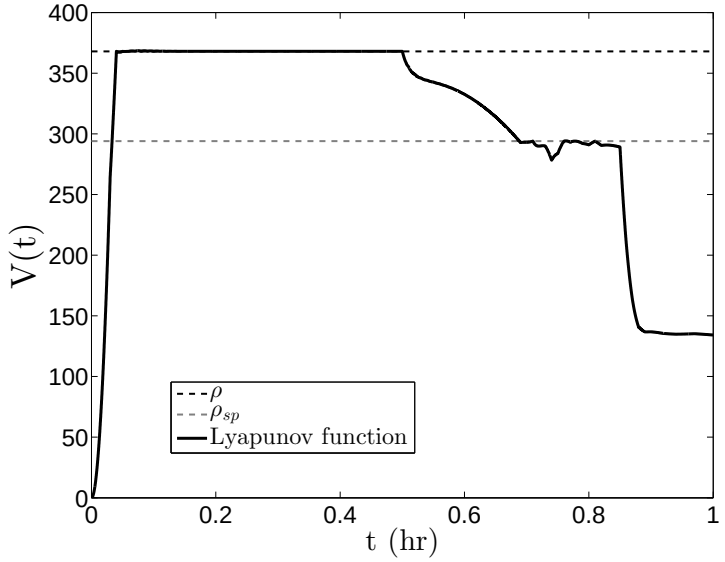

Figure 2.4: The Lyapunov function value as a function of time for the closed-loop CSTR under the stabilizing safety-LEMPC design of Eq. 2.7 (with Eq. 2.11) starting at $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho = 368$ and ending with $\rho_{sp} = 294$

bances/uncertainties (i.e., nominal process operation is considered), so the formulation for scheme 2 is presented for the case of nominal operation (i.e., for nominal operation, $\rho_e = \rho$ and no contractive constraint is needed to ensure that the state remains in Ω_ρ since we also assume $x(t_0) \in \Omega_\rho$). The second condition required to prove that scheme 2 can drive the closed-loop state from Ω_ρ into $\Omega_{\rho_{sp}}$ by t_1 is that the switching time is known in advance. The third required condition is that the time interval between the current time and t_1 is long enough in the sense that there exists an explicit stabilizing controller that can in a worst case drive the closed-loop state into $\Omega_{\rho_{sp}}$ in no more time than this time interval $t_1 - t_k$ (the remarks at the end of this section will address the use of scheme 2 when these conditions are not met). Under the assumption that these three conditions are met, the formulation of scheme 2 is as follows:

$$\max_{u\in S(\Delta)} \quad \int_{t_k}^{t_{k+\hat{N}_1+\hat{N}_2}} L_e(\tilde{x}(\tau),u(\tau))\,d\tau \tag{2.14a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t),u(t),0) \tag{2.14b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{2.14c}$$

$$u_i(t) \in U_i,\ i=1,\ldots,m,\ \forall\, t \in [t_k, t_{k+\hat{N}_1+\hat{N}_2}) \tag{2.14d}$$

$$V(\tilde{x}(t)) \leq \hat{\rho},\ \forall\, t \in [t_k, t_{k+\hat{N}_1+\hat{N}_2}) \tag{2.14e}$$

$$\hat{\rho} = \rho,\ \forall\, t \in [t_k, t_1)$$

$$\hat{\rho} = \rho_{sp},\ \forall\, t \in [t_1, t_{k+\hat{N}_1+\hat{N}_2})$$

where the prediction horizon N is the summation of two horizons $\hat{N}_1$ and $\hat{N}_2$. $\hat{N}_1$ is initially set to be the number of sampling periods required to drive the closed-loop state into the safety region and it must thus initially be equal to or less than $(t_1-t_0)/\Delta$. $\hat{N}_2$ is an additional number of sampling periods added to the prediction horizon when desired to more closely approximate the infinite-horizon case and thus, for many cases, increase the process profit by choosing control actions that optimize the cost function over a longer period of time.

In the scheme 2 safety-LEMPC formulation presented in Eq. 2.14, the long prediction horizon, region constraint, and known value of t_1 combine to drive the process state from Ω_ρ into $\Omega_{\rho_{sp}}$ by t_1. Specifically, the region constraint of Eq. 2.14 allows the nominal process to operate in a time-varying manner within the stability region Ω_ρ at the beginning of process operation. When the process has operated for a sufficient period of time (which depends on the length of the prediction horizon, including whether the initial value of $\hat{N}_1$ is equal to $(t_1-t_0)/\Delta$ or less than it) such that t_1 is within $[t_k, t_{k+\hat{N}_1+\hat{N}_2})$ (i.e., t_1 is within the prediction horizon), the region constraint of Eq. 2.14e requires that the process state be within $\Omega_{\rho_{sp}}$ by t_1 and that it remains there afterward. Thus, when the optimization problem of Eq. 2.14 is feasible, the closed-loop state is driven into $\Omega_{\rho_{sp}}$ by t_1. For nominal operation, the closed-loop process state is driven into $\Omega_{\rho_{sp}}$ and maintained there afterward,

thus accomplishing Tasks 1 and 2 of the safety-LEMPC design noted in the "Implementation strategy" section. In addition to satisfying safety constraints, all control actions calculated by scheme 2 optimize the process profit subject to the constraints.

The feasibility of the optimization problem in Eq. 2.14 can be guaranteed when the three conditions previously mentioned, which are the assumptions of nominal operation, the knowledge of t_1 in advance, and that the time interval is longer than the time that it takes a feasible (stabilizing) controller to drive the state into $\Omega_{\rho_{sp}}$ in a worst case, are met. The third requirement can be proven to hold when the initial value of $\hat{N}_1$ is equal to the number of sampling periods required in a worst-case by an explicit stabilizing controller implemented in sample-and-hold that meets the input constraints in Eq. 2.14d to drive the closed-loop state from any initial state within Ω_ρ to the safety region. However, this number of sampling periods may be large, so that a long prediction horizon may be required, even if the prediction horizon length N is set to its minimum value of $\hat{N}_1$ (i.e., $\hat{N}_2 = 0$). When the prediction horizon is long, the computation time required to solve the safety-LEMPC dynamic optimization problem may be substantially long and the controller may not be practical to implement.

Remark 2.6 *$\hat{N}_1$ is taken to be the minimum number of sampling periods required to drive the closed-loop state from any initial state in Ω_ρ into $\Omega_{\rho_{sp}}$, though it is only necessary that it is equal to the number of sampling periods required to drive the state from $x(t_1 - \hat{N}_1\Delta) \in \Omega_\rho$ to $\Omega_{\rho_{sp}}$ by t_1. However, because $x(t_1 - \hat{N}_1\Delta)$ may not be known before the controller is designed and applied, $\hat{N}_1$ should be chosen to be sufficiently large such that $x(t_1 - \hat{N}_1\Delta)$ could be any state in Ω_ρ and the process could still be driven to the safety region by t_1.*

Remark 2.7 *Because restrictive conditions are required to hold for this scheme to guarantee that the optimization problem is feasible and that the closed-loop state enters $\Omega_{\rho_{sp}}$ by t_1, this scheme may be more difficult to apply practically. However, unlike scheme 1, it has the potential to drive the closed-loop state into $\Omega_{\rho_{sp}}$ by t_1 (rather than starting to move toward $\Omega_{\rho_{sp}}$ after t_1), which may be a desirable property for processes for which changes from one region to another may need to occur by a certain time in order to ensure process safety. Thus, it may be desirable to use scheme*

2 even when the restrictive conditions (nominal operation, t_1 is known, and $t_1 - t_k$ is sufficiently long) are not known to hold. When there are disturbances, closed-loop stability and feasibility of scheme 2 cannot be proven, but they may hold. In addition, a contractive constraint like the one used in scheme 1 may be added and applied when no feasible solution is found (though this would not guarantee that the state can still be driven into $\Omega_{\rho_{sp}}$ by t_1). If t_1 is not known and thus it cannot be verified whether $t_1 - t_k$ is sufficiently long, a conservative estimate may be made of t_1, or scheme 2 may be applied long before it is expected that safety concerns may arise.

Remark 2.8 *The time that an explicit stabilizing controller $h(x)$ may take to drive the closed-loop state into $\Omega_{\rho_{sp}}$ can be estimated for a specific $h(x)$ (e.g., Sontag's controller). Specifically, the nonlinear process of Eq. 2.1 can be simulated off-line, applying $h(x)$ in a sample-and-hold fashion to measure the length of time that $h(x)$ requires to move any initial state within the stability region (i.e., $x(t_0) \in \Omega_\rho$) to the safety region.*

2.5.1 Scheme 2: Application to A Chemical Process Example

The same CSTR example that was utilized to demonstrate scheme 1 will now be used to demonstrate scheme 2 (in particular, the same steady-state, initial condition, Lyapunov function $V(x)$, Lyapunov-based controller $h(x)$, input constraints, stability region Ω_ρ, safety level set $\Omega_{\rho_{sp}}$, sampling period, and operating period were used for the process of Eq. 2.8 with the objective function of Eq. 2.10 and the material constraint of Eq. 2.11). For the demonstration of scheme 2 using this example, it is assumed that the safety logic unit indicated at the beginning of the operating period (at t_0) that it is necessary to switch the region of operation to $\Omega_{\rho_{sp}}$ where $\rho_{sp} = 294$ after half an hour (i.e., $t_1 = 0.5\ hr$, which corresponds to 50 sampling periods). As mentioned, this scheme is guaranteed to be feasible as long as the interval $t_1 - t_0$ is long enough in the sense that it is no shorter than the worst-case minimum number of sampling periods needed for a stabilizing controller that meets the input constraints and is implemented in sample-and-hold to drive the closed-loop state from the initial state within Ω_ρ to $\Omega_{\rho_{sp}}$ within $t_1 - t_0$. Because the length required for this interval is unknown without performing extensive off-line simulations as noted in Remark 2.8, the predic-

tion horizon $N = \hat{N}_1 + \hat{N}_2$ was set to 100. This ensures that if the worst-case number of sampling periods required by an explicit stabilizing controller to drive the closed-loop state into $\Omega_{\rho_{sp}}$ in the interval $t_1 - t_0$ is no more than 50 (because $(t_1 - t_0)/\Delta = 50$), the optimization problem is feasible, and the prediction horizon includes a significant number of additional sampling periods for more economically optimal process performance. The simulations demonstrated that this horizon length was sufficient, because the optimization problem was feasible. Scheme 2 was implemented with a shrinking horizon in this example (the horizon length decreases by 1 at each sampling time t_k until it becomes 0 at t_f).

The closed-loop state-space trajectories of the CSTR temperature and concentration under the scheme 2 safety-LEMPC are presented in Figure 2.5. In addition, the closed-loop trajectories of the inputs and states under scheme 2 and the corresponding values of the Lyapunov function throughout the operating window $t_f = 1\ hr$ are shown in Figure 2.6 and in Figure 2.7, respectively. The oscillatory behavior of the states and inputs observed in these figures results because scheme 2 seeks to maximize the process profit using a sufficiently long prediction horizon while still meeting process and safety constraints, and the safety-LEMPC determined that the oscillatory trajectories achieved this in the most economically optimal manner. In addition, Figure 2.5 shows the movement of the trajectories from Ω_ρ into $\Omega_{\rho_{sp}}$, and Figure 2.7 shows that the closed-loop state moved into $\Omega_{\rho_{sp}}$ by t_1 and was maintained within the safety region thereafter. Thus, scheme 2 was able to achieve economically optimal process operation while driving the closed-loop state into $\Omega_{\rho_{sp}}$ by t_1. However, despite these successes, it required a significant computation time and advance knowledge of t_1, which may not be practical in engineering applications.

2.6 Scheme 3: Simultaneous Control of Safety Constraint Sets and Process Economic Optimization

Given the drawbacks of schemes 1 and 2 of the safety-LEMPC (scheme 1 does not guarantee a fast rate of transition of the closed-loop state to the safety region, and scheme 2 requires knowledge of

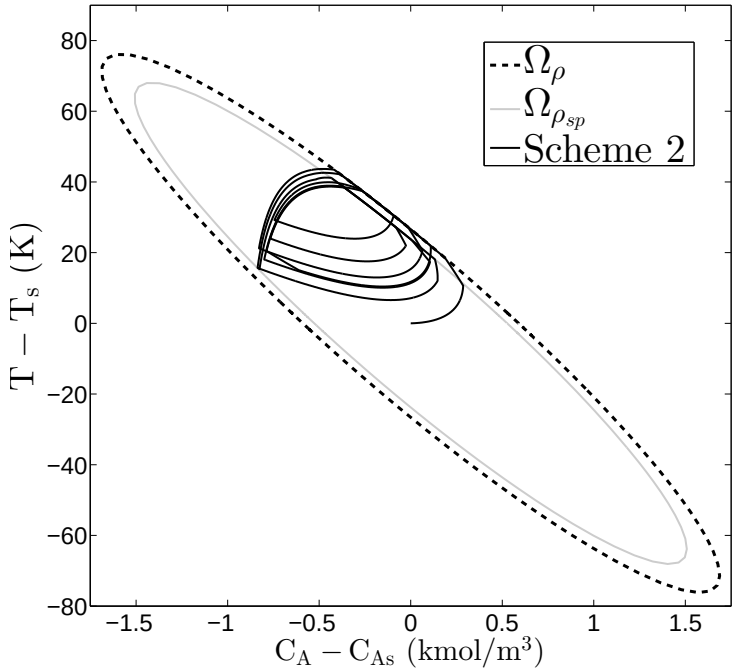

Figure 2.5: The state-space profile for the closed-loop CSTR under the long-horizon safety-LEMPC design of Eq. 2.14 (with Eq. 2.11) for the initial condition $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho = 368$

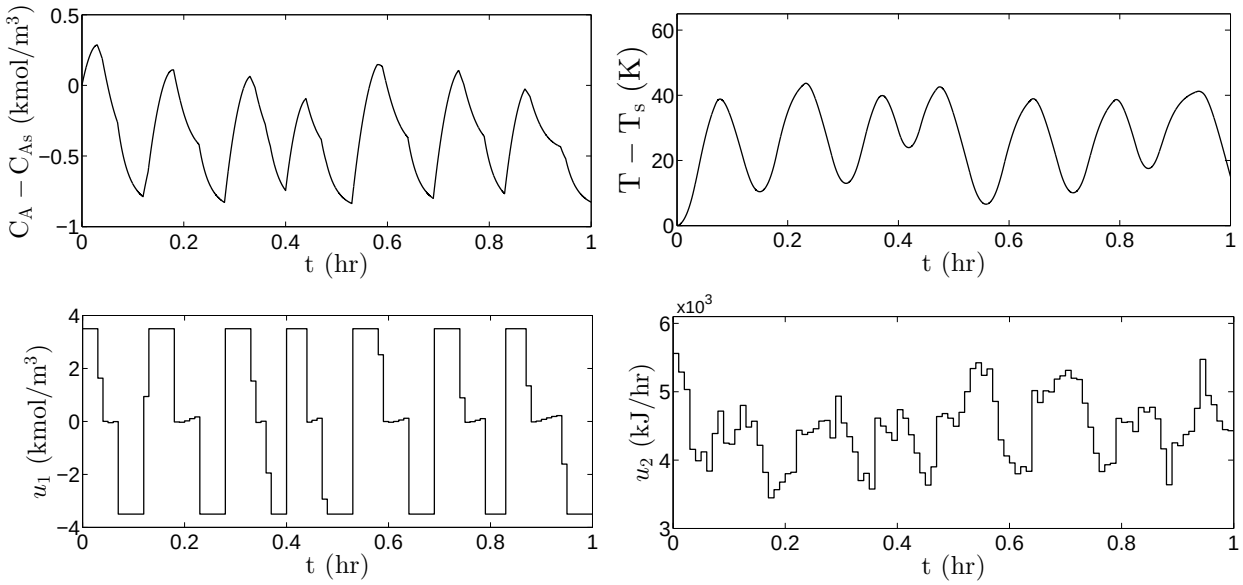

Figure 2.6: Manipulated input and state profiles for the closed-loop CSTR under the long-horizon safety-LEMPC design of Eq. 2.14 (with Eq. 2.11) for the initial condition $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$

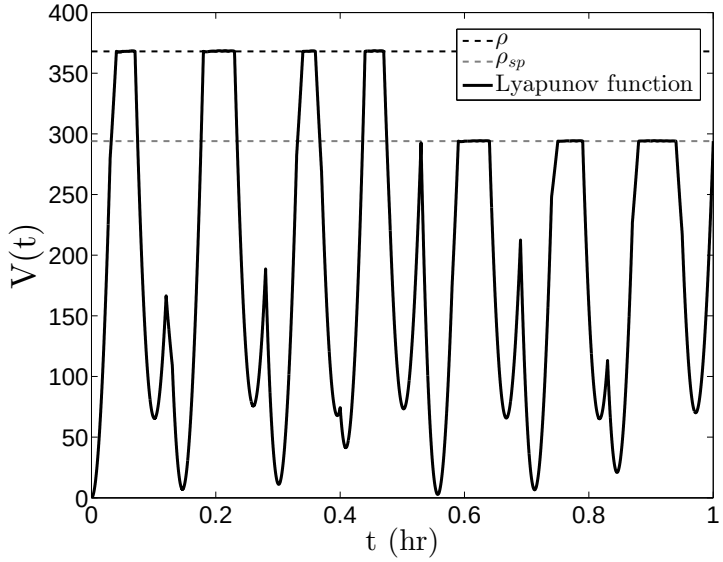

Figure 2.7: The Lyapunov function value as a function of time for the closed-loop CSTR under the long-horizon safety-LEMPC design of Eq. 2.14 (with Eq. 2.11) starting at $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho = 368$ and ending with $\rho_{sp} = 294$

the time that the closed-loop state should be within the safety region in advance and may require a long computation time), a scheme that is able to accomplish the transition of the closed-loop state between the level sets efficiently without requiring prior knowledge of the switching time was developed. This third scheme of the safety-LEMPC incorporates time-varying safety constraints (it adds auxiliary optimization variables that allow the upper bound on the Lyapunov function in the Mode 1 constraint to vary in time) and also adds a penalty in the objective with parameters that can be tuned to achieve a desired rate of transition of the closed-loop state to the safety region without the need for a long prediction horizon to ensure feasibility/stability and without requiring prior knowledge of the switching time. In this section, two formulations of scheme 3 are presented with different time-varying constraints: one that utilizes slack variables to adjust the Lyapunov function bound, and a second that decreases the upper bound on the Lyapunov function dynamically.

2.6.1 Scheme 3-1: Slack Variable Safety Level Set Constraint

In the first formulation of scheme 3, a slack variable is incorporated in the Mode 1 constraint of the LEMPC, and a penalty on the magnitude of the slack variable is imposed in the objective function

to drive the closed-loop state to the safety region at a desired rate. The scheme 3 formulation which incorporates this slack variable is presented as follows:

$$\max_{u,s\in S(\Delta)} \quad \int_{t_k}^{t_{k+N}} [L_e(\tilde{x}(\tau),u(\tau)) - a_L s(\tau)^2]\, d\tau \tag{2.15a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t),u(t),0) \tag{2.15b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{2.15c}$$

$$u_i(t) \in U_i,\ i = 1,\ldots,m,\ \forall\, t \in [t_k,t_{k+N}) \tag{2.15d}$$

$$s(t) \leq 0,\ \forall\, t \in [t_k,t_{k+N}) \text{ if } t_k \geq t_1 \text{ and } x(t_k) \notin \Omega_{\rho_{sp}} \tag{2.15e}$$

$$s(t) = 0,\ \forall\, t \in [t_k,t_{k+N}) \text{ if } t_k < t_1, \text{ or if } t_k \geq t_1 \text{ and } x(t_k) \in \Omega_{\rho_{sp}} \tag{2.15f}$$

$$V(\tilde{x}(t)) + s(t) \leq \hat{\rho},\ \forall\, t \in [t_k,t_{k+N}) \tag{2.15g}$$

$$\hat{\rho} = \rho,\ \forall\, t \in [t_k,t_{k+N}) \text{ if } t_k < t_1$$

$$\hat{\rho} = \rho_{sp},\ \forall\, t \in [t_k,t_{k+N}) \text{ if } t_k \geq t_1$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k),u(t_k),0) \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k),h(x(t_k)),0) \tag{2.15h}$$

$$\text{if } x(t_k) \notin \Omega_{\rho_e} \text{ and } t_k < t_1 \text{ or } x(t_k) \notin \Omega_{\bar{\rho}_{sp}} \text{ and } t_k \geq t_1$$

where s denotes the piecewise constant slack variable of the optimization problem over the prediction horizon $N\Delta$, and a_L is a weighting constant.

From the formulation of scheme 3 in Eq. 2.15, it can be seen that like scheme 1, scheme 3 optimizes the process economics within Ω_ρ until t_1. The slack variable is set to $s(t) = 0$ in Eq. 2.15f before t_1, so the safety-LEMPC reduces to the standard formulation of LEMPC in Eq. 2.6 with an additional modification (not noted in Eq. 2.15 to avoid complicating the notation that $\hat{\rho}$ is set to ρ_e before t_1). At t_1, the safety constraints of Eqs. 2.15e, 2.15g, and 2.15h are activated. Thus, at t_1, the contractive constraint of Eq. 2.15h begins to be enforced, and it is enforced until the closed-loop state enters $\Omega_{\bar{\rho}_{sp}}$ to ensure that the Lyapunov function always decreases between

two sampling periods when the closed-loop state is outside $\Omega_{\bar{\rho}_{sp}}$ (this ensures that Tasks 1 and 2 of the safety-LEMPC strategy from the "Implementation strategy" section are accomplished). In addition, the upper bound $\hat{\rho}$ in Eq. 2.15g is changed to ρ_{sp} at t_1, and the slack variable is allowed to take negative values. The role of the slack variable in this constraint is to ensure feasibility of the optimization problem. If the slack variable was not included in Eq. 2.15g, the optimization problem may be infeasible at t_1 because the closed-loop state was allowed to vary throughout all of Ω_ρ before t_1, and thus it would not in general be expected that $x(t_1) \in \Omega_{\rho_{sp}}$. Because of this, the slack variable, which takes a negative value per Eq. 2.15e, is added to the value of $V(\tilde{x}(t))$, $t \in [t_k, t_{k+N})$ to decrease the left-hand side of Eq. 2.15g so that the upper bound ρ_{sp} can be met. Thus, this scheme enforces the decrease of the Lyapunov function level set as a soft constraint.

An important role of the slack variable is to ensure feasibility of the optimization problem when the safety logic unit requires the region of operation to change. The second role of the slack variable is to cause the safety-LEMPC to compute control actions that drive the closed-loop state into $\Omega_{\rho_{sp}}$ as quickly as possible when desired. This is a result of its appearance in the objective of Eq. 2.15a as a term that decreases the value of the objective function and thus it causes the safety-LEMPC to seek control actions that make the magnitude of $s(t)$ as small as possible to maximize the objective function value when the weighting constant a_L is sufficiently large. From Eq. 2.15g, the magnitude of $s(t)$ will be smaller as $V(\tilde{x}(t))$ becomes closer to ρ_{sp}, and finally takes its minimum magnitude of zero when $V(x(t_k)) = \rho_{sp}$. Thus, for a sufficiently large a_L, the use of the slack variable dictates scheme 3-1 to choose control actions that improve the rate of transition to $\Omega_{\rho_{sp}}$ compared to the rate which would be obtained if only the contractive constraint of Eq. 2.15h were used. The rate of decrease of the level set value is adjusted by varying the weighting constant a_L.

Remark 2.9 *a_L is a weighting constant that determines the rate at which the closed-loop state goes to $\Omega_{\rho_{sp}}$ by penalizing the magnitude of the slack variable in the objective. Due to the penalty in the objective function and the constraint of Eq. 2.15g, the optimal value of the slack variable at each sampling time when $t_k \geq t_1$ and $x(t_k) \notin \Omega_{\rho_{sp}}$ will be equal to $\rho_{sp} - V(\tilde{x}(t_j))$, where $\tilde{x}(t_j)$*

is the predicted state that gives the maximum value of the Lyapunov function in a given sampling period. If it is desired to move quickly toward the safety region regardless of whether or not this decreases the process profit, then a_L must be sufficiently large in the sense that it must dominate the economics-based component $L_e(\tilde{x},u)$ of the objective function.

Remark 2.10 *The formulation of Eq. 2.15 implements the slack variable carefully so that issues with closed-loop stability cannot occur due to the slack variable. In this remark, we clarify some of the important aspects of the formulation in Eq. 2.15. Firstly, the reason that $s(t)=0$ when the state is not transitioning between Ω_ρ and $\Omega_{\rho_{sp}}$ is that if a_L is small, there is a potential that the economic benefit of increasing the magnitude of $s(t)$ to operate the process in a larger region of operation may outweigh the loss in the objective function from the addition of the term containing the slack variable (as an extreme case, a_L may be set to 0 if it is desired to only optimize the process economics, and then the slack variable magnitude may become arbitrarily large to maximize the economics). By setting $s(t)=0$ when the state is within the safety region, such issues cannot occur during operation within the safety region. When the state is transitioning to the safety region, the use of the contractive constraint throughout the transition period ensures that none of the implemented control actions (i.e., the control actions corresponding to the first sampling period in the prediction horizon) will cause the closed-loop state to leave Ω_ρ or to move away from the safety level set, regardless of the values of a_L and of $s(t)$, $t\in[t_k,t_{k+N})$; however, it cannot be guaranteed that control actions for the remaining $N-1$ sampling periods of the prediction horizon (for which the contractive constraint is not imposed) will not cause undesirable behavior for $s(t)$, $t\in[t_{k+1},t_{k+N})$ if a_L is small. Because these $N-1$ control actions are never implemented, their behavior cannot affect whether the implemented control actions move the state to a lower level set, but it may affect the economic optimality or constraint satisfaction of the process if, for example, constraints that depend on past control actions are included (and if infeasibility occurs, such that even the contractive constraint is not satisfied by the LEMPC solution, it may be necessary to use a different controller such as the Lyapunov-based controller to ensure that the state can be driven to lower level sets, though this may not satisfy process constraints). Therefore, it is necessary to*

tune a_L carefully or, if there are concerns that it cannot be tuned in such a way to guarantee that the slack variables do not pose an issue for the process, the contractive constraint of Eq. 2.15h can be enforced at each sampling period of the prediction horizon, which will ensure that all predicted control actions decrease the value of the Lyapunov function and can prevent infeasibility in later sampling periods if the optimization problem is properly formulated. If this issue is accounted for, a_L can be tuned to achieve the desired rate of approach to the safety region. If a_L = 0, the slack variable formulation puts more emphasis on the optimization of economics during the approach to the safety region than the speed of approach to the safety region; as a_L is increased, the slack variable formulation will drive the state more quickly to the safety region, within the possible speed of the dynamics of the process and any state/input constraints. An advantage of this slack variable formulation over scheme 1 is that it has greater flexibility because it can be used to maximize profit during the approach to the safety region or used for the alternate purpose of improving the speed of approach to the safety region; a disadvantage, however, is that it requires the addition of additional optimization variables to do so, which may increase the computation time.

Remark 2.11 *In the formulation in Eq. 2.15, the slack variable is shown as a negative number added to the left-hand side of Eq. 2.15g to decrease the left-hand side to be below ρ_{sp} after t_1. An alternative way to consider this constraint is to instead require that the slack variables be positive, and to add them to the right-hand side of Eq. 2.15g, instead of to the left. This increases the bound on the right-hand side so that the value of the Lyapunov function at $\tilde{x}(t)$ is within this upper bound.*

Remark 2.12 *In the formulation of Eq. 2.15, the slack variable $s(t)$ is calculated at every sampling period in the prediction horizon. However, one may consider updating $s(t)$ less often than once per sampling period (e.g., having one slack variable for the entire prediction horizon) to reduce the number of optimization variables, since only the first control action of the prediction horizon is applied. However, a careful analysis should be performed when one slack variable is used over the prediction horizon due to the bound $\rho_{sp} - V(\tilde{x}(t_j))$ on the slack variable that was mentioned in Remark 2.9. To further clarify, this bound implies that if one slack variable is used for the entire prediction horizon and it is desired to move the closed-loop state to the safety region quickly (i.e.,*

a_L is large), then depending on how this constraint is imposed in the controller, the slack variable $s(t)$ may be ineffective at accomplishing its purpose of causing the implemented control action to move the closed-loop state from Ω_ρ to $\Omega_{\rho_{sp}}$ at a rate faster than that given by the Lyapunov-based controller.

To see this, consider first the extreme case in which the constraint of Eq. 2.15g is enforced at every time instance in the prediction horizon, including the sampling time t_k at the beginning of the prediction horizon, when the state is transitioning from Ω_ρ to $\Omega_{\rho_{sp}}$. However, $s(t)$ takes only one value for $t \in [t_k, t_{k+N})$ since we are considering the case that one slack variable is used for the whole prediction horizon. In a best case, the value of the Lyapunov function will never become greater than its initial value $V(x(t_k))$ throughout the prediction horizon because it is desired to move all predicted control actions toward the safety level set. Then, because the constraint of Eq. 2.15g must be satisfied at t_k since it is enforced at that time, and the value of $V(x(t_k))$ is the maximum value of $V(\tilde{x}(t))$ throughout the prediction horizon, the controller will choose $s(t) = \rho_{sp} - V(x(t_k))$, $t \in [t_k, t_{k+N})$ to make the bound of Eq. 2.15g as tight as possible to minimize the value of $s(t)$ and maximize the objective (since a_L is large). This means that the value of the slack variable is set by the measured state $x(t_k)$, which is not able to be adjusted by the controller, so the penalty term in the objective becomes a constant depending on a measured value of the closed-loop state and thus is ineffective at driving the state into $\Omega_{\rho_{sp}}$ as quickly as possible (the objective in this case is equivalent to using only $L_e(\tilde{x}, u)$, so as for scheme 1, the maximization of economics during the approach to the safety region will slow the approach). Since the Lyapunov function decreases throughout the first sampling period due to the contractive constraint of Eq. 2.15h and only the first sampling period of the prediction horizon is implemented on the process, it is desirable to make the value of the Lyapunov function at the end of the first sampling period as small as possible to move the closed-loop state as quickly as possible to the safety region, which can be obtained by enforcing the constraint of Eq. 2.15g at the end of the first sampling period, rather than at any other point during that sampling period.

Scheme 3-1: Application to A Chemical Process Example

To demonstrate scheme 3-1, the formulation of Eq. 2.15 (with the added material constraint) was applied to the same CSTR example that was utilized previously to demonstrate schemes 1 and 2. The optimization variables were the manipulated inputs as well as one slack variable that was held constant throughout the prediction horizon $N = 10$ (one slack variable was used to avoid having a large number of optimization variables that might increase the computation time as in scheme 2). The weighting coefficient was chosen to be $a_L = 80$ to severely penalize the slack variable term in the objective function when the closed-loop state is transitioning between Ω_ρ and $\Omega_{\rho_{sp}}$. Due to this significant weight, the constraint of Eq. 2.15e was enforced for all times (Eq. 2.15f was not used).

In this demonstration of scheme 3-1, the process is initially operated in Ω_ρ. After half an hour of operation in Ω_ρ, it is assumed that the safety logic unit determines that it is necessary to switch to the safety region $\Omega_{\rho_{sp}}$ ($t_1 = 0.5\ hr$). After t_1, the safety-LEMPC calculates control actions that quickly drive the closed-loop state into $\Omega_{\rho_{sp}}$ due to the significant penalty term on the magnitude of the slack variable in the objective function. Figures 2.8, 2.9, and 2.10 depict the state-space trajectories, state and input trajectories, and Lyapunov function value, respectively, for the CSTR operated under scheme 3-1. Figure 2.8 shows the transition of the closed-loop state from Ω_ρ into $\Omega_{\rho_{sp}}$, and Figure 2.10 shows that the controller was able to drive the closed-loop state into the safety region in 2 sampling periods after t_1 and maintain it within the safety region thereafter. From these figures, it is observed that scheme 3-1 effectively drove the state to the desired safety region rapidly. In addition, this scheme was not computationally expensive and did not require prior knowledge of the switching time.

Remark 2.13 *Based on the discussion in Remark 2.12, it should be noted that the one slack variable in this example was implemented by enforcing the Mode 1 constraint at the end of each sampling period of the prediction horizon to avoid the issues noted in that remark.*

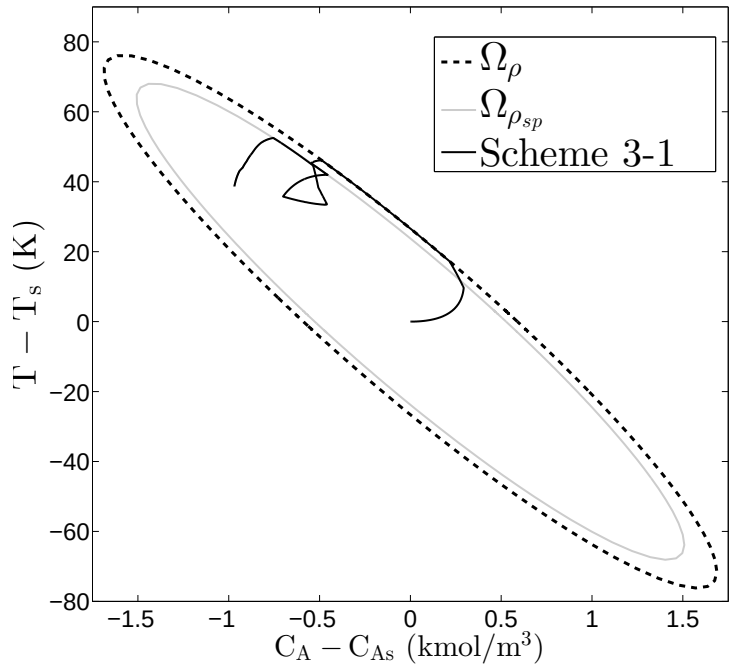

Figure 2.8: The state-space profile for the closed-loop CSTR under the slack variable safety-LEMPC design of Eq. 2.15 (with Eq. 2.11) for the initial condition $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho = 368$

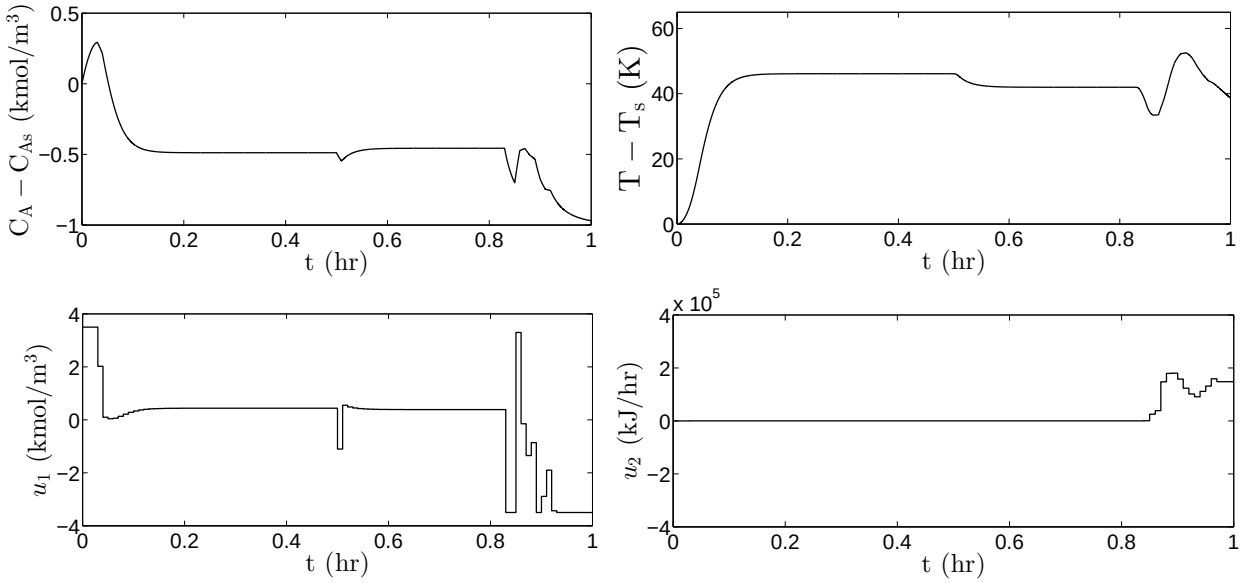

Figure 2.9: Manipulated input and state profiles for the closed-loop CSTR under the slack variable safety-LEMPC design of Eq. 2.15 (with Eq. 2.11) for the initial condition $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$

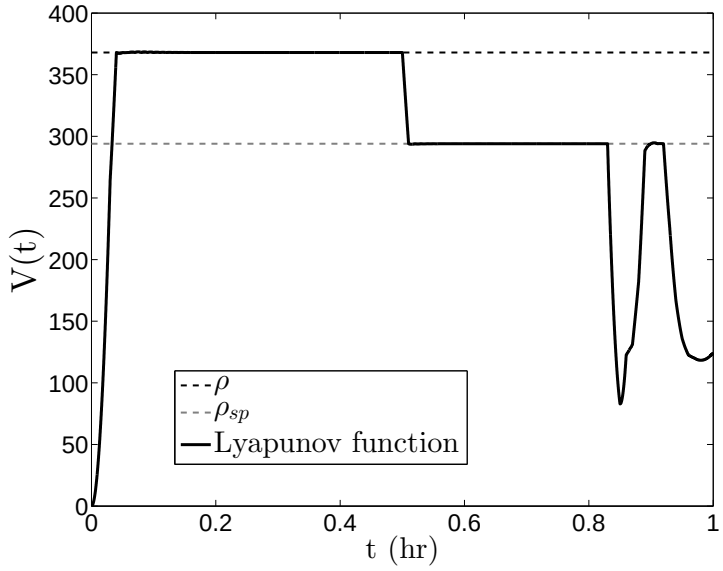

Figure 2.10: The Lyapunov function value as a function of time for the closed-loop CSTR under the slack variable safety-LEMPC design of Eq. 2.15 (with Eq. 2.11) starting at $[C_A(0), T(0)] = [1.2\ \frac{kmol}{m^3}, 438\ K]$ and $\rho = 368$ and ending with $\rho_{sp} = 294$

2.6.2 Scheme 3-2: Dynamic Safety Level Set (DSLS)

The motivation of the second formulation of scheme 3, termed dynamic safety level set-LEMPC (DSLS-LEMPC), is to design a controller that explicitly controls the rate at which the closed-loop state goes to the safety region $\Omega_{\rho_{sp}}$ while maximizing the process economics. The DSLS-LEMPC design utilizes the explicit stabilizing controller $h(x)$ and dynamic safety-based constraints that decrease the upper bound on the Lyapunov function through an ordinary differential equation to drive the closed-loop state into the safety region at a desired rate while maintaining closed-loop stability and recursive feasibility of the system of Eq. 2.1 under the DSLS-LEMPC design in the presence of uncertainty. In addition to optimizing the process economic performance, the DSLS-LEMPC paradigm, like the other schemes presented, performs Tasks 1 and 2 of the safety-LEMPC noted in the "Implementation Strategy" section.

The optimization problem of the proposed DSLS-LEMPC for the process of Eq. 2.1 is pre-

sented for the case that t_1 has been reached, and is as follows:

$$\max_{u(t),K_c(t)\in S(\Delta)} \int_{t_k}^{t_{k+N}} [L_e(\tilde{x}(\tau),u(\tau)) - \phi(\rho_{sp} - \tilde{\rho}(\tau))]d\tau \tag{2.16a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t),u(t),0) \tag{2.16b}$$

$$u_i(t) \in U_i,\ i = 1,\ldots,m,\ \forall\, t \in [t_k, t_{k+N}) \tag{2.16c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{2.16d}$$

$$K_c(t) \geq 0\ , \forall\, t \in [t_k, t_{k+N}) \tag{2.16e}$$

$$V(\tilde{x}(t)) \leq \tilde{\rho}(t),\ \forall\, t \in [t_k, t_{k+N}) \tag{2.16f}$$

$$\frac{d\tilde{\rho}}{dt} = K_c(t)(\rho_{sp} - \tilde{\rho}(t)) \tag{2.16g}$$

$$\begin{aligned} &\tilde{\rho}(t_k) = V(x(t_k)), \quad \text{if } x(t_k) \notin \Omega_{\rho_{sp}} \\ &\tilde{\rho}(t_k) = \rho_{sp}, \quad \text{if } x(t_k) \in \Omega_{\rho_{sp}} \end{aligned} \tag{2.16h}$$

$$\begin{aligned} &\frac{\partial V(x(t_k))}{\partial x} f(x(t_k),u(t_k),0) \\ &\quad \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k),h(x(t_k)),0), \\ &\qquad \text{if } x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}} \text{ or } t_k > t_s \end{aligned} \tag{2.16i}$$

where t_s is the time after which the DSLS-LEMPC starts to drive the closed-loop state into a small neighborhood of the origin in the presence of disturbances, which will be elaborated upon in the "Feasibility and stability analysis" section (in the previous safety-LEMPC schemes, t_s was not included for simplicity of presentation and thus was assumed to be infinity; it has been included here to simplify the discussion of the feasibility and closed-loop stability properties of the safety-LEMPC's that will be given in the "Feasibility and stability analysis" section based on this scheme 3-2 formulation). In addition to the manipulated input $u(t)$, the piecewise constant gain $K_c(t)$ is a decision variable of the optimization problem defined over the prediction horizon $N\Delta$. The function $\phi(\cdot)$ is appropriately chosen to give a desired rate of approach of the closed-loop state to $\Omega_{\rho_{sp}}$ (it may be, for example, the squared absolute value of its arguments). The constraint of Eq.

2.16e restricts the gain $K_c(t)$ to take nonnegative values over the prediction horizon. The DSLS-LEMPC optimization problem minimizes the stage cost $L_e(\tilde{x}(\tau), u(\tau))$, derived from the system economics, and the penalty $\phi(\rho_{sp} - \tilde{\rho}(t))$ that penalizes the deviation of the upper bound of the Lyapunov function value $\tilde{\rho}(t)$ from the safety set-point ρ_{sp} over the prediction horizon.

The dynamic safety-based constraints in Eqs. 2.16e-2.16h control the rate of variation of the level set of the predicted Lyapunov function value $V(\tilde{x}(t))$ over the prediction horizon to shrink the region of operation to $\Omega_{\rho_{sp}}$. Specifically, the constraint of Eq. 2.16f maintains the predicted state trajectory $\tilde{x}(t)$ in the region $\Omega_{\tilde{\rho}(t)}$ over the prediction horizon. The level set $\Omega_{\tilde{\rho}(t)}$ of the predicted Lyapunov function changes with time through the first order differential equation of Eq. 2.16g. The gain $K_c(t)$ adjusts the rate of decrease of the level set $\Omega_{\tilde{\rho}(t)}$ over the prediction horizon. The initial condition of Eq. 2.16g is obtained from the value of the Lyapunov function at the current state if the current state is outside the safety region $\Omega_{\rho_{sp}}$; however, if the current state enters the safety region (i.e., $x(t_k) \in \Omega_{\rho_{sp}}$) then the initial condition will be set to the safety set-point ρ_{sp} (Eq. 2.16h). The contractive constraint (Eq. 2.16i) forces the control actions computed by the DSLS-LEMPC to decrease the Lyapunov function for the first sampling period in the prediction horizon by at least as much as the decrease given by the explicit stabilizing controller $h(x)$. Because of the safety-based constraints and the contractive constraint, it is guaranteed that the Lyapunov function value will decrease for the first sampling period (i.e., $V(x(t_{k+1})) \leq V(x(t_k))$). This continuous decreasing of the Lyapunov function value guarantees that the closed-loop state will be driven into the safety region in finite time, which accomplishes Task 1 of the safety-LEMPC. Moreover, to achieve boundedness of the closed-loop state within the safety region $\Omega_{\rho_{sp}}$ and thus, meet the requirement of Task 2, the contractive constraint of Eq. 2.16i will force the closed-loop state into the subset of the safety region $\Omega_{\bar{\rho}_{sp}} \subset \Omega_{\rho_{sp}}$ which makes the region $\Omega_{\rho_{sp}}$ a forward invariant set.

Remark 2.14 *The contractive constraint of Eq. 2.16i is imposed in the optimization problem to ensure that $\tilde{\rho}(t)$ is decreasing at the beginning of each sampling period t_k in the presence of disturbances, and the role of the constraints in Eqs. 2.16e-2.16h in this case is to enhance the rate of decrease of $\tilde{\rho}(t)$ over the prediction horizon. However, the constraints of Eqs. 2.16e-2.16h will*

decrease $\tilde{\rho}(t)$ without the need to impose the contractive constraint (Eq. 2.16i) for the nominal system of Eq. 2.1 (i.e., $w(t) \equiv 0$) under the DSLS-LEMPC design when the gain $K_c(t)$ is sufficiently large over the prediction horizon.

Remark 2.15 *Owing to the constraint of Eq. 2.16h, the penalty term $\phi(\rho_{sp} - \tilde{\rho}(t))$ in the objective function of the optimization problem of Eq. 2.16 will be equal to zero and the upper bound of the predicted Lyapunov function value in Eq. 2.16f will be set to the safety set-point ρ_{sp} once $x(t_k)$ enters the safety region $\Omega_{\rho_{sp}}$. From that point on, due to the contractive constraint of Eq. 2.16i, $\Omega_{\rho_{sp}}$ will be a forward invariant set if $\Omega_{\bar{\rho}_{sp}}$ is defined such that no state starting within $\Omega_{\bar{\rho}_{sp}}$ can leave $\Omega_{\rho_{sp}}$ in a sampling period (which will be proven in the "Feasibility and stability analysis" section).*

Remark 2.16 *If the penalty term $\phi(\rho_{sp} - \tilde{\rho}(t))$ is large relative to the process economic cost, it will be desirable that $\tilde{\rho}(t) = \rho_{sp}$, which means that it is preferable to go as quickly as possible to $\Omega_{\rho_{sp}}$ and then optimize the profit after the closed-loop state enters the safety region, rather than optimizing it along the way. Thus, the weighting on the economics-based part of the objective function compared to that of the safety-based penalty may depend on the process and how long in advance of a fault or change in the process conditions the controller is notified that it needs to change the region of operation to $\Omega_{\rho_{sp}}$.*

Remark 2.17 *Note that the decrease of $\tilde{\rho}(t)$ through Eq. 2.16g does not mean that the value of the Lyapunov function of the actual state $V(x(t))$ has decreased according to Eq. 2.16g. This is due to process disturbances and also the fact that $V(x)$ is a separate function for which the dynamics are not those in Eq. 2.16g. However, if $K_c(t)$ and $u(t)$ can be found that can decrease $\tilde{\rho}(t)$ in Eq. 2.16f, the predicted state is guaranteed to be within smaller level sets. If $\tilde{\rho}(t)$ decreases quickly, this means that there is a value of $u(t)$ that can quickly decrease $V(\tilde{x}(t))$ and thus may decrease $V(x(t))$ significantly, even if it is not able to decrease it by as much as is indicated by Eq. 2.16f due to disturbances in the actual process.*

Remark 2.18 *Unlike the piecewise constant input $u(t)$ which is, for practical implementation reasons, implemented in a sample-and-hold fashion, $K_c(t)$ can be updated as often as desired because it is an auxiliary variable for optimization purposes and not a control action that is implemented by the actuator, and thus there is no limit on how often it can be updated; however, constant updating (e.g., every integration step) in general is not computationally practical.*

Remark 2.19 *It was noted that the DSLS-LEMPC formulation was presented for the case that t_1 had already been reached, and it is desired to move the state into $\Omega_{\rho_{sp}}$, to provide better clarity to the discussion of the scheme by explicitly including ρ_{sp} in the formulation of Eq. 2.16. In the time before t_1, the value of $\bar{\rho}_{sp}$ in Eq. 2.16i would be replaced by ρ_e, and the upper bound on $V(\tilde{x}(t))$ would be set to ρ_e instead of $\tilde{\rho}$ in Eq. 2.16f. At t_1, the EMPC of Eq. 2.16 would then be used as written, which would require only an update of the values of ρ_{sp} and $\bar{\rho}_{sp}$ from the safety logic unit.*

Remark 2.20 *Scheme 3-1 and scheme 3-2 have many similarities and can be used to accomplish similar goals, though they are not equivalent. They both have the benefit of flexibility compared to schemes 1 and 2 because of the tuning parameters that they incorporate, as noted for scheme 3-1 in Remark 2.10. Like scheme 3-1, a disadvantage of scheme 3-2 compared to schemes 1 and 2 is that it requires the addition of auxiliary decision variables that may increase the computation time.*

There are several differences in the manner in which schemes 3-1 and 3-2 handle the dynamic variation of the upper bound on the Lyapunov function throughout time. For example, the auxiliary optimization variable $K_c(t)$ used in scheme 3-2 is not included in any equation that includes the values of the closed-loop states themselves, but is only used to modify the bound on the Lyapunov function. In addition, it is not utilized in the objective function, so there are no possible negative interactions between $K_c(t)$ and the values of the closed-loop states that would require $K_c(t)$ to be set to a specific value once the state enters the safety region. This is in contrast to scheme 3-1, where the slack variable $s(t)$ is used in the Mode 1 constraint that is also a function of the states and thus can directly affect their values, in addition to being in the objective. This can cause the competing effects noted in Remark 2.10 that require $s(t)$ to be set to 0 after the state

enters the safety region. Another significant difference between the two schemes is that scheme 3-2 controls the upper bound on the Lyapunov function value through the first-order ordinary differential equation that adjusts the bound on the Lyapunov function value $\tilde{\rho}(t)$ in time. Though this differential equation requires a value of the decision variable $K_c(t)$ to modify the Lyapunov function bound, the bound on the Lyapunov function value is not directly calculated by the safety-LEMPC. Thus, scheme 3-2 can be described as adjusting the bound on the level set by using a controller (Eq. 2.16g) within the safety-LEMPC controller. In contrast, scheme 3-1 modifies the upper bound on the Lyapunov function by adjusting $s(t)$, which is an optimization variable of the safety-LEMPC.

Another difference between the two formulations is that if it is desired to reduce the computation time by applying only one value of the auxiliary variable ($s(t)$ in scheme 3-1 and $K_c(t)$ in scheme 3-2) throughout the prediction horizon, the manner in which $s(t)$ is implemented in such a case is an important consideration in scheme 3-1, as noted in Remark 2.12, due to the structure of that optimization problem, but no special considerations need to be made for scheme 3-2. On the other hand, there may be some benefit with respect to the rate of approach of the closed-loop state to the safety region when the number of optimization variables $K_c(t)$ in scheme 3-2 is increased (i.e., there are more decision variables $K_c(t)$ than the number of sampling periods in the prediction horizon) due to the increase in flexibility that this may give to adjust the upper bound on the Lyapunov function $\tilde{\rho}(t)$ (and thus the greater possibility of finding control actions that move the state to the safety region more quickly). For scheme 3-1, in contrast, there is no benefit to increasing the number of slack variables $s(t)$ because the slack variables set the upper bound on the Lyapunov function directly and when the input is piecewise constant as in the safety-LEMPC schemes, changing the upper bound on the Lyapunov function often throughout a sampling period will not affect the values of the control actions chosen since they are fixed throughout the sampling period.

Remark 2.21 *Unlike scheme 2, schemes 3-1 and 3-2 do not guarantee that the closed-loop state will be within $\Omega_{\rho_{sp}}$ by any specific time. They can be tuned to drive the state into $\Omega_{\rho_{sp}}$ quickly in*

the sense that they may take the minimum or close to the minimum number of sampling periods possible to drive the closed-loop state into $\Omega_{\rho_{sp}}$ from $x(t_1)$; however, the actual speed of this transition will depend on the process dynamics and state/input constraints, and thus may not, in practice, occur on a short timescale. Scheme 2 had the benefit then that regardless of the speed of the process dynamics and constraints, it can drive the state into $\Omega_{\rho_{sp}}$ by a required time; however, it is not in general possible to prove that it can do this in the presence of disturbances or if t_1 is not known, whereas schemes 3-1 and 3-2 are robust to disturbances and require no prior knowledge of the switching time.

Remark 2.22 *There are no restrictions on the objective functions that can be used with the safety-LEMPC schemes. This means that they hold not only for an economics-based objective, but can also hold for traditional quadratic objectives utilized in tracking MPC in industry. An elaboration of this will be the subject of the next chapter.*

Scheme 3-2: Application to A Chemical Process Example

The DSLS-LEMPC design is demonstrated using the same CSTR example that was used for scheme 1, scheme 2 and scheme 3-1, but with different problem settings. Specifically, the process of Eq. 2.8 was operated with the same objective function in Eq. 2.10, the same constraints on the inputs, for $t_f = 1\ hr$, using a prediction horizon $N = 10$ and a sampling period $\Delta = 0.01\ hr$. However, the material constraint of Eq. 2.11 was not used. The process of Eq. 2.8 was operated around the unstable steady-state point $[C_{As2}\ T_{s2}]$=[2 $\frac{kmol}{m^3}$ 400 K]. Moreover, a quadratic Lyapunov function $V(x) = x^T Px$ was constructed with $P = \text{diag}([636.94\ 0.5])$ to determine the stability region Ω_ρ for the DSLS-LEMPC design. The weights of the P matrix were chosen so that each state contributed to the Lyapunov function value approximately equally. The stability region was chosen to be the largest level set where the time-derivative of the Lyapunov function, $\dot{V}$, along the closed-loop state trajectories is negative under the Lyapunov-based controller $h(x) = [h_1(x)\ h_2(x)]^T$

defined by feedback linearization as follows:

$$h_1(x) = \frac{V}{F}[-\gamma x_1 + \frac{-F}{V}(C_{A0s} - (x_1 + C_{As2})) + k_0 e^{\frac{-E}{R(x_2+T_{s2})}}(x_1 + C_{As2})^2]$$

$$h_2(x) = \rho_L C_p V[-\gamma x_2 + \frac{-F}{V}(T_0 - (x_2 + T_{s2})) + \frac{\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{R(x_2+T_{s2})}}(C_{As2} + x_1)^2]$$

where $\gamma = 25$ was chosen to make the process model of Eq. 2.8 globally exponentially stable under $h(x)$ in the absence of input constraints. Both control laws are subject to the input constraints and by using this strategy, ρ was chosen to be 2002.3.

The change in the example specifications in this section is made to show that the safety-LEMPC schemes have the potential not only to ensure safe operation around a stable steady-state, but also around an unstable steady-state. The examples presented in this chapter are not intended to be used to directly compare the performance of the schemes for the particular system used, but rather to demonstrate the properties of the individual schemes, since the objective of this chapter is to develop several safety-LEMPC schemes and to present their differences and similarities so that a control engineer can have an understanding of which scheme may be best for a particular application due to its properties as a formulation.

We assume that at the beginning of operation the safety logic unit determines that it is necessary to shift the region of operation Ω_ρ to the safety region $\Omega_{\rho_{sp}}$ where $\rho_{sp} = 500$ (i.e., $t_1 = t_0$), again to reduce the maximum allowable temperature of operation. The process of Eq. 2.8 is controlled by the DSLS-LEMPC design given by the following optimization problem:

$$\min_{u\in S(\Delta),K_c} \int_{t_k}^{t_{k+N}} \left[\frac{-L_e(\tilde{x}(\tau),u(\tau))}{N\Delta} + \frac{|\rho_{sp}-\tilde{\rho}(\tau)|^2}{h_c} \right] d\tau \tag{2.18a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t),u(t),0) \tag{2.18b}$$

$$u_i(t) \in U_i,\ i=1,\ldots,m,\ \forall\, t\in[t_k,t_{k+N}) \tag{2.18c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{2.18d}$$

$$K_c \geq 0,\ \forall\, t\in[t_k,t_{k+N}) \tag{2.18e}$$

$$V(\tilde{x}(t)) \leq \tilde{\rho}(t),\ \forall\, t\in[t_k,t_{k+N}), \tag{2.18f}$$

$$\frac{d\tilde{\rho}}{dt} = K_c(\rho_{sp}-\tilde{\rho}(t)) \tag{2.18g}$$

$$\tilde{\rho}(t_k) = V(x(t_k)), \quad \text{if } x(t_k)\notin\Omega_{\rho_{sp}}$$

$$\tilde{\rho}(t_k) = \rho_{sp}, \quad \text{if } x(t_k)\in\Omega_{\rho_{sp}} \tag{2.18h}$$

where the optimization variables are the piecewise-constant trajectory for $u(t)$ and the auxiliary optimization variable K_c (only one value of K_c is found for the entire prediction horizon to minimize the number of auxiliary optimization variables used), and h_c is the integration time step 10^{-5} hr.

The DSLS-LEMPC formulation considered is implemented with a prediction horizon $N=10$. The objective function of the optimization problem includes two terms; the first term is the negative of the time-average production rate of Eq. 2.10 (to maximize the production rate since Eq. 2.18 is a minimization problem), and the second term is the L^2 norm of the difference between $\tilde{\rho}(t)$ and the safety set-point ρ_{sp}. We penalize the second term significantly more than the average production rate using a large weight $1/h_c$ so that the highest priority of the DSLS-LEMPC is to drive the closed-loop state into the safety region $\Omega_{\rho_{sp}}$ in a short time.

In the following simulation, we demonstrate the application of the proposed DSLS-LEMPC by starting the optimization problem from an initial condition that is at the boundary of stability region Ω_ρ (significantly far from the safety region) to assess the quality of the DSLS-LEMPC controller. Figures 2.11-2.12 show the closed-loop state trajectories and the manipulated input trajectories of

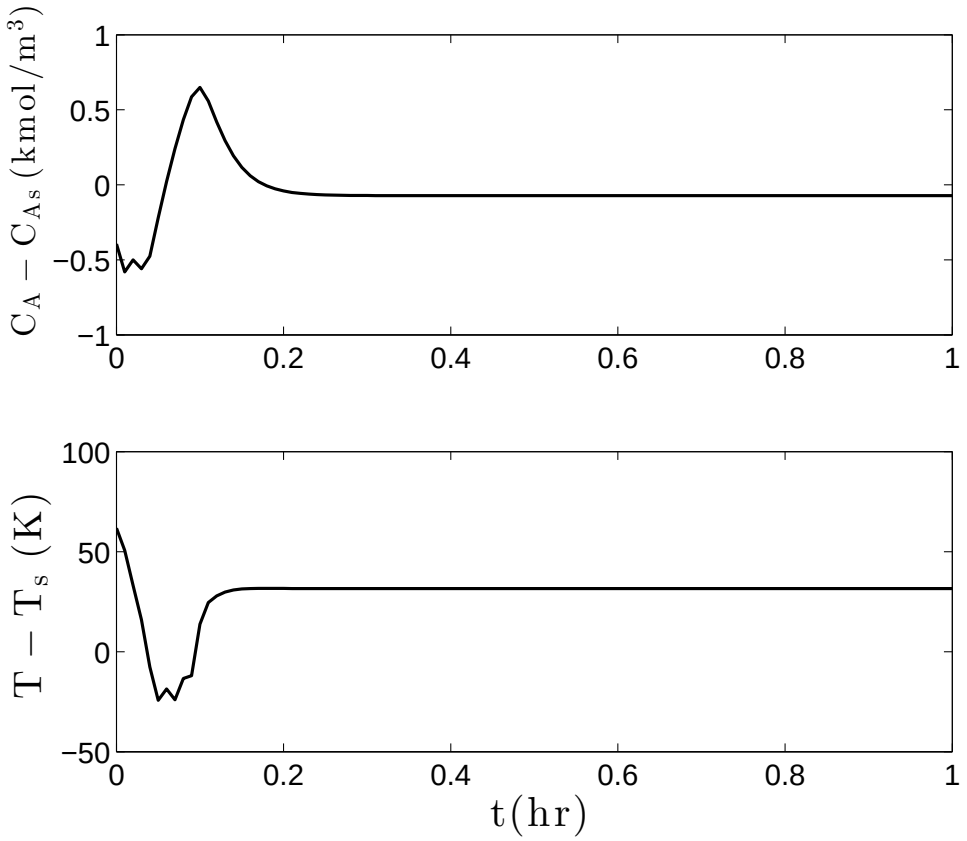

Figure 2.11: The state profiles for the closed-loop CSTR under the DSLS-LEMPC design of Eq. 2.18 for the initial condition $[C_A(0), T(0)] = [1.606\ \frac{kmol}{m^3}, 461.7\ K]$

the dynamic model of Eq. 2.8 under the DSLS-LEMPC design of Eq. 2.18. Due to the high penalty in the objective function on the deviation of the predicted states from the safety region $\Omega_{\rho_{sp}}$, the manipulated heat rate u_2 drops to its minimum allowable value at the beginning of the operating period to decrease the temperature of the reactor x_2 as quickly as possible so that the closed-loop trajectories enter the safety region in a short time. Once the closed-loop state trajectories are inside the safety region $\Omega_{\rho_{sp}}$, the objective function reduces to only the average production rate, so the inlet concentration u_1 saturates at its maximum allowable value to increase the reactant concentration x_1, and thus the profit is maximized. The DSLS-LEMPC controller was able to drive the closed-loop state trajectories into the safety region $\Omega_{\rho_{sp}}$ within three sampling periods (i.e., 3Δ). Another simulation was performed to demonstrate that the DSLS-LEMPC is efficient at adapting to sudden changes of the safety set-point. In this simulation, the safety logic unit required

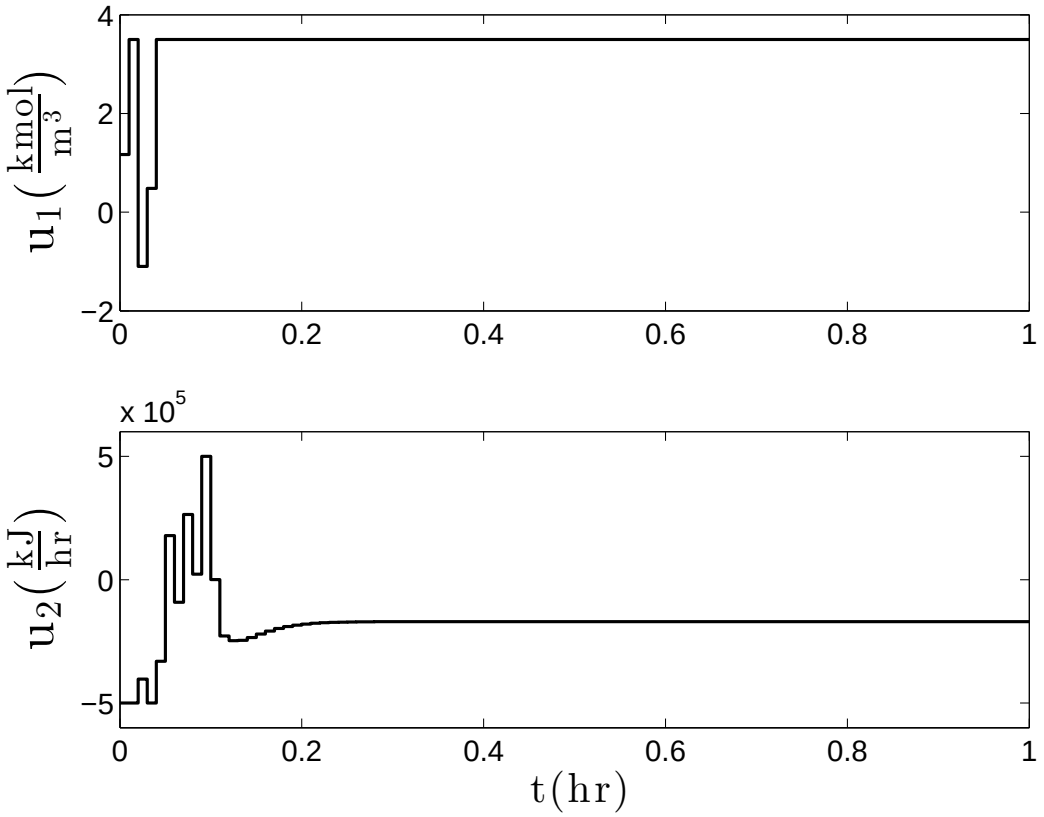

Figure 2.12: Manipulated input profiles for the closed-loop CSTR under the DSLS-LEMPC design of Eq. 2.18 for the initial condition $[C_A(0), T(0)] = [1.606\ \frac{kmol}{m^3}, 461.7\ K]$

the process state to move to two different safety level sets at two different time instants, where $t_1 = t_0$ and $t_2 = 0.5\ hr$, with the corresponding safety set-points being $\rho_{sp_1} = 500$ and $\rho_{sp_2} = 300$. Figure 2.13 represents the state trajectory in this case; clearly the DSLS-LEMPC was successfully able to drive the closed-loop state into the boundary of $\Omega_{\rho_{sp_2}}$ within one sampling period after t_2 where the process state settled to maximize the profit.

Figure 2.14 depicts the closed-loop state-space trajectories for x_1 and x_2 starting from an initial level set $\Omega_{\rho_{int}}$ that is equal to the level set Ω_ρ (i.e., $\rho = \rho_{int} = V(x(t_0))$, where t_0 is the initial time). As shown in Figure 2.14, shortly after the closed-loop state trajectories enter the safety region, they start to approach the boundary of the safety region to maximize the production rate. Also, the state trajectories settle at the point $[x_1(0), x_2(0)] = [0.07\ \frac{kmol}{m^3}, 31.53\ K]$ where the production rate attains a local maximum within the specified safety region $\Omega_{\rho_{sp}}$.

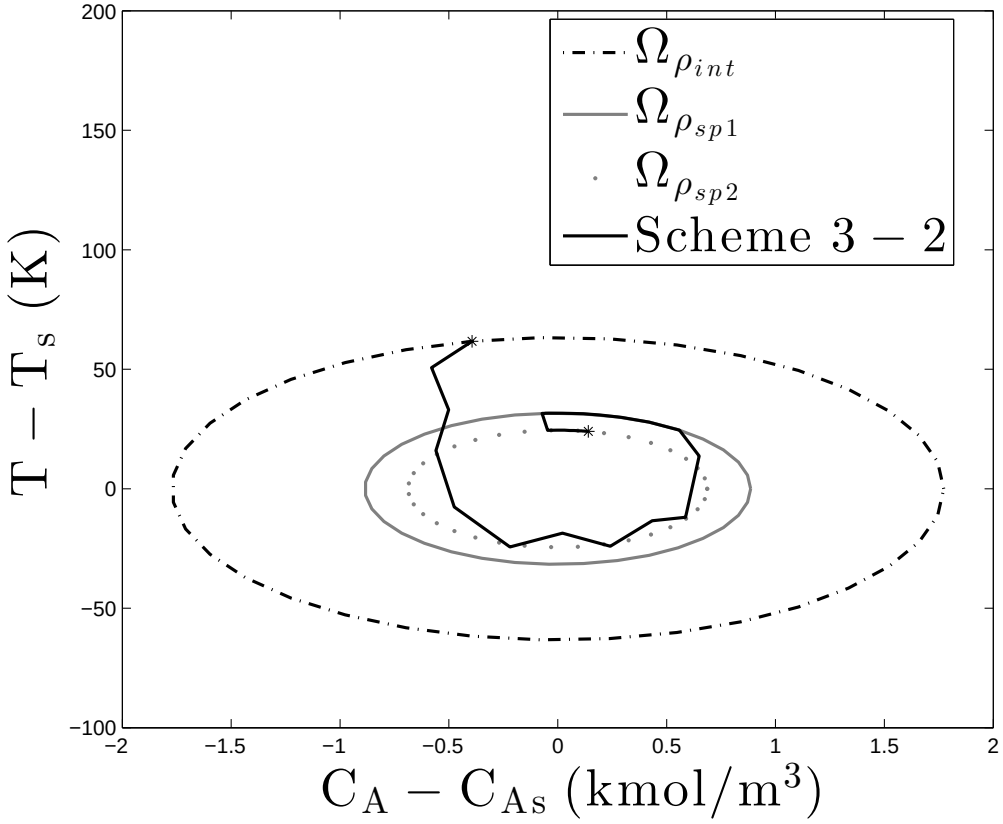

Figure 2.13: The state-space profile for the closed-loop CSTR under the DSLS-LEMPC design of Eq. 2.18 for the initial condition $[C_A(0), T(0)] = [1.606\ \frac{kmol}{m^3}, 461.7\ K]$ and $\rho_{int} = 2002.3$ for two different safety set-points $\rho_{sp1} = 500$ at $t_1 = 0$ *hr*, $\rho_{sp2} = 300$ at $t_2 = 0.5$ *hr*

Figure 2.15 shows the inverse relationship between the gain $K_c(t)$ and the initial value of $\tilde{\rho}(t)$ of Eq. 2.18g at the beginning of each sampling period t_k under the DSLS-LEMPC design of Eq. 2.18. The gain $K_c(t)$ levels off at a constant value after the initial value of $\tilde{\rho}(t)$ of Eq. 2.18g under the DSLS-LEMPC is equal to the safety set-point value $\rho_{sp} = 500$.

Remark 2.23 *The formulation of the DSLS-LEMPC used for this example, shown in Eq. 2.18, is not guaranteed to be stabilizing in the sense of convergence to a small neighborhood of the steady-state, particularly around the unstable steady-state, since it does not include the contractive constraint for simplicity. It was able to maintain the closed-loop state within the stability region in the simulations discussed above; to guarantee convergence to a small neighborhood of the steady-state or robustness to disturbances in this example, the contractive constraint should be added.*

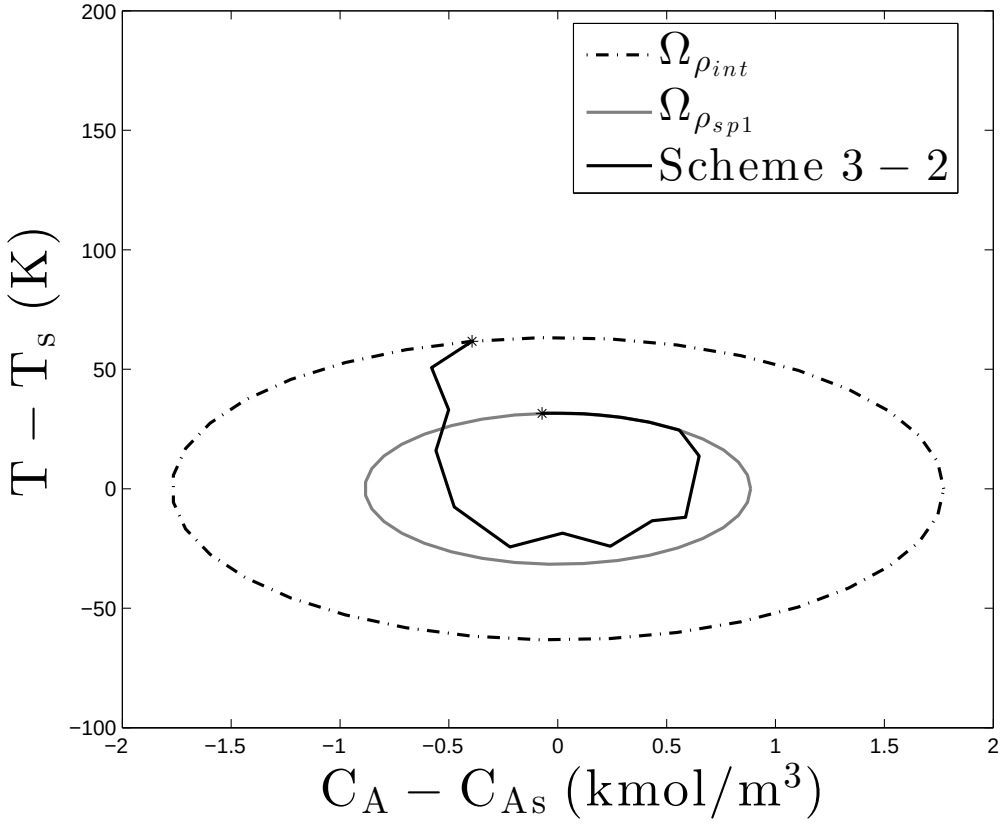

Figure 2.14: The state-space profile for the closed-loop CSTR under the DSLS-LEMPC design of Eq. 2.18 for the initial condition $[C_A(0), T(0)] = [1.606\ \frac{kmol}{m^3}, 461.7\ K]$ and $\rho_{int} = 2002.3$

2.6.3 Feasibility and Stability Analysis

In this section, we present sufficient conditions such that the state of the closed-loop system of Eq. 2.1 under the three safety-LEMPC schemes is always bounded in $\Omega_{\rho_{sp}}$ and is ultimately bounded in a compact set containing the origin. We present these results in detail for the DSLS-LEMPC design, and then describe how they can be generalized to the other safety-LEMPC schemes through several remarks. Since the DSLS-LEMPC design is a modified formulation of the classical LEMPC design of,[43] the proofs of stability and feasibility utilize the approach in.[43] We begin the proof for the DSLS-LEMPC by re-stating the two propositions required for stability and feasibility from[43] to define functions and parameters needed for the proof of feasibility and closed-loop stability of the DSLS-LEMPC formulation.

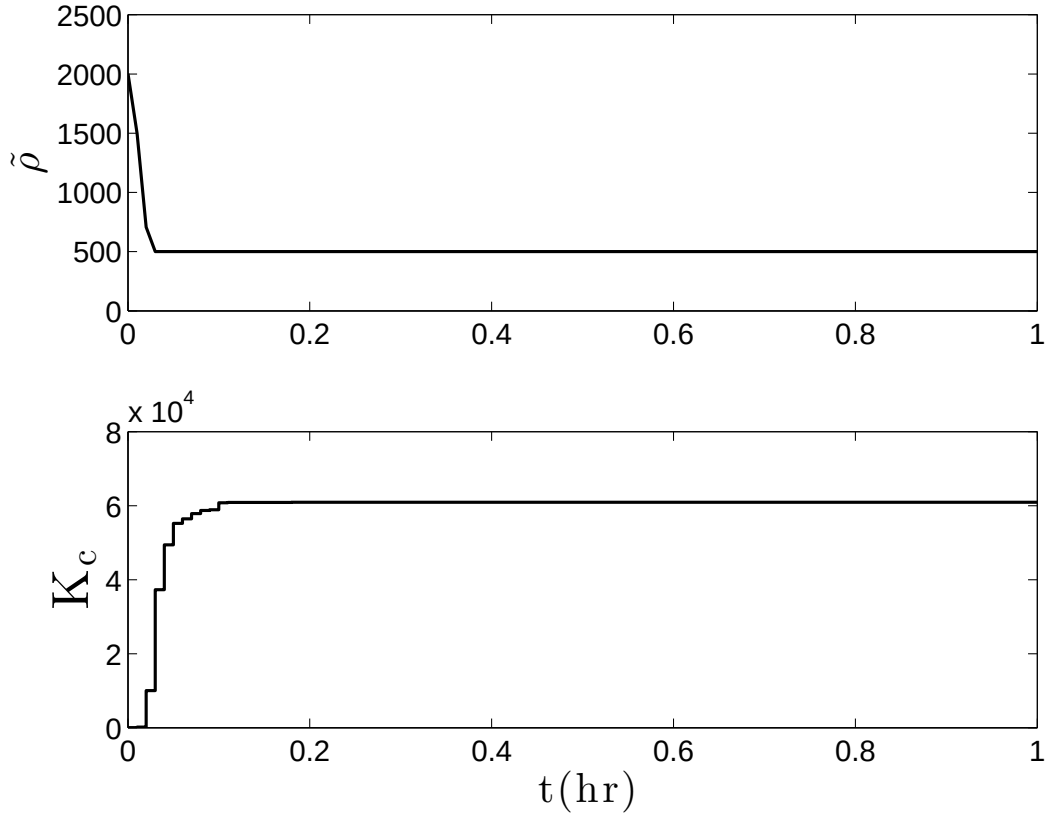

Figure 2.15: The gain K_c and the initial value of $\tilde{\rho}(t)$ of Eq. 2.18g at the beginning of each sampling period t_k for the closed-loop CSTR under the DSLS-LEMPC design of Eq. 2.18 for the initial condition $[C_A(0), T(0)] = [1.606\ \frac{kmol}{m^3}, 461.7\ K]$

Proposition 2.1 (c.f.[43,67]) *Consider the systems*

$$\begin{aligned} \dot{x}_a(t) &= f(x_a(t), u_1(t), \ldots, u_m(t), w(t)) \\ \dot{x}_b(t) &= f(x_b(t), u_1(t), \ldots, u_m(t), 0) \end{aligned} \tag{2.19}$$

with initial states $x_a(t_0) = x_b(t_0) \in \Omega_\rho$. There exists a $\mathscr{K}$ function $f_W(\cdot)$ such that

$$|x_a(t) - x_b(t)| \leq f_W(t - t_0), \tag{2.20}$$

for all $x_a(t), x_b(t) \in \Omega_\rho$ and all $w(t) \in W$ with

$$f_W(\tau) = \frac{L_w \theta}{L_x}(e^{L_x \tau} - 1). \tag{2.21}$$

Proposition 2.2 (c.f.[43,67]) *Consider the Lyapunov function $V(\cdot)$ of the system of Eq. 2.1. There exists a quadratic function $f_V(\cdot)$ such that*

$$V(x) \leq V(\hat{x}) + f_V(|x-\hat{x}|) \tag{2.22}$$

for all $x, \hat{x} \in \Omega_\rho$ with

$$f_V(s) = \alpha_4(\alpha_1^{-1}(\rho))s + M_v s^2 \tag{2.23}$$

where M_v is a positive constant.

In the following theorem, we establish feasibility and stability of DSLS-LEMPC by introducing conditions on ρ_{sp} and $\bar{\rho}_{sp}$.

Theorem 2.1 *Consider the system of Eq. 2.1 in closed-loop under the DSLS-LEMPC design of Eq. 2.16 based on a controller $h(x)$ that satisfies the conditions of Eq. 2.2. Let $\varepsilon_w > 0$, $\Delta > 0$, $\rho > \rho_{sp} > \bar{\rho}_{sp} > \rho_s > 0$ satisfy*

$$\bar{\rho}_{sp} \leq \rho_{sp} - f_V(f_W(\Delta)) \tag{2.24}$$

and

$$-\alpha_3(\alpha_2^{-1}(\rho_s)) + L_x' M\Delta + L_w'\theta \leq -\varepsilon_w/\Delta. \tag{2.25}$$

If $x(t_0) \in \Omega_\rho$, $\rho_{\min} \leq \bar{\rho}_{sp}$ and $N \geq 1$ where

$$\rho_{\min} = \max\{V(x(t+\Delta)) : V(x(t)) \leq \rho_s\}, \tag{2.26}$$

then the state $x(t)$ of the closed-loop system can be driven in a finite time to $\Omega_{\rho_{sp}}$ and then be bounded there, and also the state $x(t)$ of the closed-loop system is ultimately bounded in $\Omega_{\rho_{\min}}$.

Proof 2.1 *The proof will be given in two parts. In Part 1, we prove the feasibility of the optimization problem of Eq. 2.16 for all initial states starting within the region Ω_ρ. In Part 2, we prove the two results of Theorem 2.1 (which are that the state $x(t)$ of the closed-loop system can be driven in a finite time to $\Omega_{\rho_{sp}}$ and then be bounded there, and also is ultimately bounded in $\Omega_{\rho_{\min}}$).*

Part 1: The solution $K_c(t) = 0, \forall\, t \in [t_k, t_{k+N})$, $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$ *with* $n = k, \ldots, N+k-1$ *is a feasible solution when* $\tilde{x}(t)$ *is maintained within* Ω_ρ. *The gain* $K_c(t) = 0, \forall\, t \in [t_k, t_{k+N})$ *is feasible since it satisfies Eq. 2.16e over the prediction horizon. When* $K_c(t) = 0$, *then by Eq. 2.16g,* $\tilde{\rho}(t)$ *will be equal to its initial value from Eq. 2.16h throughout the prediction horizon, and thus the upper bound on the Lyapunov function in Eq. 2.16f will be fixed (i.e., either* $\tilde{\rho}(t_k) = V(x(t_k)) \Rightarrow V(\tilde{x}(t)) \leq V(x(t_k)), \forall\, t \in [t_k, t_{k+N})$, *if* $x(t_k) \notin \Omega_{\rho_{sp}}$ *or* $\tilde{\rho}(t_k) = \rho_{sp} \Rightarrow V(\tilde{x}(t)) \leq \rho_{sp}, \forall\, t \in [t_k, t_{k+N})$, *if* $x(t_k) \in \Omega_{\rho_{sp}}$*). In such a case, the feasibility of* $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$ *with* $n = k, \ldots, N+k-1$ *is guaranteed because it satisfies the input constraint of Eq. 2.16c and also, because of the closed-loop stability property of the Lyapunov-based controller* $h(x)$[72] *(when Eqs. 2.25-2.26 are met for the process under both* $h(x)$ *and under the LEMPC of Eq. 2.16), it satisfies the constraint of Eq. 2.16f. Trivially,* $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$ *with* $n = k, \ldots, N+k-1$ *satisfies the contractive constraint of Eq. 2.16i, making it a feasible input trajectory for the DSLS-LEMPC design of Eq. 2.16. Therefore,* $K_c(t) = 0, \forall\, t \in [t_k, t_{k+N})$, $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$ *with* $n = k, \ldots, N+k-1$ *is a feasible solution, and recursive feasibility of the DSLS-LEMPC follows if the closed-loop state trajectory is maintained within* Ω_ρ *(which will be proven in Part 2).*

Part 2: We now show that if the closed-loop state $x(t_k)$ *is initialized outside the safety region (i.e.,* $x(t_k) \notin \Omega_{\rho_{sp}}$ *and* $t_k \leq t_s$*), then within finite time the closed-loop state will be maintained in* $\Omega_{\rho_{sp}}$. *We also show that if* $t_k > t_s$, *then the closed-loop state will be ultimately bounded in a small region containing the origin.*

If $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$, *then due to the contractive constraint of Eq. 2.16i in the DSLS-LEMPC formulation of Eq. 2.16, the Lyapunov function of the closed-loop state will decrease for the first sampling period in the prediction horizon by at least the rate given by the explicit stabilizing controller* $h(x)$. *Owing to the closed-loop stability property of the explicit controller* $h(x)$,[72] *the Lyapunov function value of the closed-loop state under the DSLS-LEMPC design will decrease in the next sampling period (i.e.,* $V(x(t)) \leq V(x(t_k)), \forall\, t \in [t_k, t_{k+1}]$, *which is derived in*[43]*). Thus, if* $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$ *then* $V(x(t_{k+1})) < V(x(t_k))$ *and in finite time, the closed-loop state converges to* $\Omega_{\bar{\rho}_{sp}}$ *(i.e.,* $x(t_{k+j}) \in \Omega_{\bar{\rho}_{sp}}$ *where* j *is a finite positive integer).*

When the closed-loop state enters $\Omega_{\rho_{sp}}$, the upper bound of the constraint in Eq. 2.16f is replaced by $\bar{\rho}_{sp}$, then for $x(t_k) \in \Omega_{\bar{\rho}_{sp}}$ and $t_k \leq t_s$, then $\tilde{x}(t_{k+1}) \in \Omega_{\bar{\rho}_{sp}}$ by the constraints of Eq. 2.16f and $x(t_{k+1}) \in \Omega_{\rho_{sp}}$ (also, $x(t) \in \Omega_{\rho_{sp}}$ for $t \in [t_k, t_{k+1})$) because the contractive constraint will only not be applied to decrease the Lyapunov function value if $x(t_k) \notin \Omega_{\bar{\rho}_{sp}}$, it is also possible to execute the EMPC formulation of Eq. 2.16 as written and to guarantee that $x(t_{k+1}) \in \Omega_{\rho_{sp}}$ for all times if $\Omega_{\bar{\rho}_{sp}}$ is defined as a region chosen such that if $x(t_k) \in \Omega_{\bar{\rho}_{sp}}$, then $x(t) \in \Omega_{\rho_{sp}}$) for $t \in [t_k, t_{k+1})$). If $x(t_k) \in \Omega_{\rho_{sp}}/\Omega_{\bar{\rho}_{sp}}$, then the contractive constraint will continue to be enforced, decreasing the Lyapunov function value until $x(t_{k+l}) \in \Omega_{\bar{\rho}_{sp}}$ where l is a finite positive integer. Therefore, $\Omega_{\rho_{sp}}$ is a forward invariant set.

If $t_k > t_s$, then the contractive constraint of Eq. 2.16i will continue to decrease the Lyapunov function value until the closed-loop state enters the compact set $\Omega_{\rho_{min}}$ in which it is ultimately bounded. The proof of this is analogous to the proof of ultimate boundedness in.[43]

Remark 2.24 *As noted in Remark 2.19, before t_1, the safety-LEMPC operates with ρ and ρ_e replacing ρ_{sp} and $\bar{\rho}_{sp}$ in the formulation of Eq. 2.16, so scheme 3-2 is also stable before t_1 and ensures closed-loop stability for the same reasons as mentioned in the proof of Theorem 2.1.*

Remark 2.25 *The proofs of feasibility and closed-loop stability of schemes 1, 2, and 3-1, under the assumptions of Theorem 2.1 that $\Omega_{\rho_{min}} \subseteq \Omega_{\bar{\rho}_{sp}}$ and that $x(t_0) \in \Omega_{\rho}$, have many similarities to the proof presented for the DSLS-LEMPC and will be outlined in several following remarks. These remarks will show that schemes 1 and 3-1, like scheme 3-2, have robustness properties that guarantee that they can maintain closed-loop stability of the process state within a given safety region in the presence of sufficiently small disturbances (i.e., disturbances small enough that the Lyapunov-based controller implemented in sample-and-hold is robust to these disturbances) after the state has entered this safety region, and will show that scheme 2 can guarantee that the closed-loop state can be maintained within a given safety region for nominal operation.*

Remark 2.26 *For scheme 1, $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$ with $n = k, \ldots, N+k-1$, is a feasible solution when $t_k < t_1$ and when $t_k \geq t_1$ because it satisfies the input constraints and the Mode 1 and*

Mode 2 constraints in Eqs. 2.7c, 2.7d, and 2.7e. This scheme is also guaranteed to maintain closed-loop stability of the state before and after t_1. Before t_1, $\hat{\rho} = \rho_e$, and the safety-LEMPC operates as the standard LEMPC in Eq. 2.6, which is guaranteed to maintain closed-loop stability according to the proof presented in.[43] From t_1 until the state first enters $\Omega_{\bar{\rho}_{sp}}$, the Mode 2 constraint of Eq. 2.7e is able to drive the closed-loop state from any state in Ω_ρ into $\Omega_{\bar{\rho}_{sp}}$ because of the robustness property of the explicit stabilizing controller, as mentioned in the proof of Theorem 2.1 for the DSLS-LEMPC. Finally, after the state has reached $\Omega_{\bar{\rho}_{sp}}$, it is maintained within this final level set by the combination of the Mode 1 and Mode 2 constraints in the same manner as was detailed for the DSLS-LEMPC in the proof of Theorem 2.1.

Remark 2.27 *Feasibility and closed-loop stability for scheme 2 can be proven when the three conditions mentioned in the section "Scheme 2: LEMPC with sufficiently long prediction horizon" are met (nominal process operation, t_1 is known, and the time interval $t_1 - t_k$ is longer than $t_1 - \hat{N}_1\Delta$, where $\hat{N}_1$ is defined based on an explicit stabilizing controller $h(x)$). When these conditions are met, $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$ with $n = k, \ldots, N+k-1$ is a feasible solution because it is guaranteed to drive the closed-loop state from $x(t_0) \in \Omega_\rho$ to $\Omega_{\rho_{min}}$ in finite time if implemented repeatedly due to the stability properties of the Lyapunov-based controller.[72] Thus, before t_1 is within the prediction horizon, $\hat{\rho} = \rho$ in Eq. 2.14e and $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$ with $n = k, \ldots, N+k-1$ is a feasible solution because it decreases the value of $V(x(t))$ with time which ensures that $V(\tilde{x}(t))$ is maintained within Ω_ρ. When t_1 is within the prediction horizon (and thus $\hat{\rho} = \rho$ before t_1 and ρ_{sp} starting at t_1 in Eq. 2.14e), $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$ with $n = k, \ldots, N+k-1$ is feasible because the prediction horizon was designed with respect to $h(x)$ to be at least as long as the time needed for an explicit stabilizing controller $h(x)$ implemented in sample-and-hold to drive the closed-loop state into $\Omega_{\rho_{sp}}$ in a worst case from any point within Ω_ρ while meeting the input constraints of Eq. 2.14d. Closed-loop stability in the sense of boundedness of the closed-loop state within Ω_ρ before it enters $\Omega_{\rho_{sp}}$ and within $\Omega_{\rho_{sp}}$ after it first enters the safety region is guaranteed for a nominal process operated under scheme 2 when a feasible solution exists because then the constraints of Eq. 2.14e hold not only in the optimization problem but also for the actual process.*

Remark 2.28 *For scheme 3-1,* $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$, $n = k, \ldots, N+k-1$, *with* $s(t) = 0\ \forall\ t \in [t_k, t_{k+N})$ *is a feasible solution before* t_1 *because it trivially satisfies the contractive constraint and Eq. 2.15f and also satisfies the constraint of Eq. 2.15g because* $\hat{\rho} = \rho$. *When* $t_k \geq t_1$ *and* $x(t_k) \notin \Omega_{\rho_{sp}}$, $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$, $n = k, \ldots, N+k-1$, *with a negative* $s(t)$ *of arbitrarily large magnitude allows for Eqs. 2.15e and 2.15g to be satisfied and also satisfies the contractive constraint and the input constraints by design of* $h(x)$. *When* $t_k \geq t_1$ *and* $x(t_k) \in \Omega_{\rho_{sp}}$, $\hat{\rho} = \rho_{sp}$, *and* $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$, $n = k, \ldots, N+k-1$, *with* $s(t) = 0\ \forall\ t \in [t_k, t_{k+N})$ *is a feasible solution because it again satisfies both the contractive constraint and the constraints of Eqs. 2.15g and 2.15f. The proof of the closed-loop stability of this method follows that of the standard LEMPC of Eq. 2.6 presented in*[43] *before* t_1. *Scheme 3-1 decreases the state to* $\Omega_{\bar{\rho}_{sp}}$ *in finite time due to the contractive constraint and then maintains the state within* $\Omega_{\rho_{sp}}$ *after it enters this set for the reasons described for the DSLS-LEMPC in the proof of Theorem 2.1.*

Remark 2.29 *To prove ultimate boundedness of the closed-loop state under schemes 1 and 3-1, the contractive constraint in each scheme could be enforced for all times after a pre-specified time* t_s. *To prove ultimate boundedness of the closed-loop state under scheme 2, this contractive constraint could be added to scheme 2 at* t_s *and enforced for all times after* t_s. *In all three cases, the proof of ultimate boundedness would follow that presented for the DSLS-LEMPC in Part 2 of the proof of Theorem 2.1.*

2.7 Conclusion

In this chapter, safety-LEMPC schemes were introduced to combine feedback control, process economics and safety considerations. Three different safety-LEMPC schemes that maintain safe operation while maximizing the profit were developed. The first scheme used a contractive constraint to compute control actions that drive the closed-loop state to a safe region of operation at least as quickly as a stabilizing Lyapunov-based controller would in a worst-case. However, under this scheme, the rate of the transition between the regions of operation may be slow. Though

the second scheme utilized a sufficiently long prediction horizon and a region constraint to ensure that the state was within the safety region by a specific time, it may require a long computation time associated with the larger number of decision variables required to simulate a process over a long prediction horizon. The third scheme tackled the drawbacks of the first two schemes by giving two formulations that incorporate time-varying safety-based constraints to transition the closed-loop state between the regions of operation efficiently. The first formulation incorporated a slack variable to achieve this while the second formulation (DSLS-LEMPC) dynamically controlled the upper bound on the Lyapunov function directly. For a sufficiently small sampling period, we proved recursive feasibility and closed-loop stability of a class of nonlinear systems under the safety-LEMPC schemes for nominal operation and, for schemes 1 and 3, in the presence of uncertainty. A chemical process example under each of the safety-LEMPC schemes was presented to demonstrate the ability of the proposed controllers to drive the closed-loop state into a safe region of operation and then maintain it within the safety region while maximizing the profit of the process. Closed-loop stability was maintained in all simulations and the safety-LEMPC schemes demonstrated an effective economic performance and safety constraints satisfaction.

Chapter 3

Achieving Operational Process Safety via Model Predictive Control

3.1 Introduction

An MPC formulation (which can be considered to be an EMPC formulation with, specifically, a quadratic objective function) that can guarantee closed-loop stability in the presence of uncertainty is Lyapunov-based model predictive control (LMPC) which incorporates stability constraints based on a stabilizing Lyapunov-based controller. Though LMPC drives the closed-loop state trajectory to a steady-state, it lacks the ability to adjust the rate at which the closed-loop state approaches the steady-state in an explicit manner. However, there may be circumstances in which it would be desirable, for safety reasons, to be able to adjust this rate to avoid triggering of safety alarms or process shut-down. In addition, there maybe scenarios in which the current region of operation is no longer safe to operate within, and another region of operation (i.e., a region around another steady-state) is appropriate. Motivated by these considerations, this chapter develops two novel LMPC schemes by extending the results from the prior chapter that can drive the closed-loop state to a safety region (a level set within the stability region where process functional safety is ensured) at a prescribed rate or can drive the closed-loop state to a safe level set within the stability re-

gion of another steady-state. Recursive feasibility and closed-loop stability are established for a sufficiently small LMPC sampling period. A comparison between the proposed method, which effectively integrates feedback control and safety considerations, and the classical LMPC method is demonstrated with a chemical process example. The chemical process example demonstrates that the safety-LMPC drives the closed-loop state into a safe level set of the stability region two sampling times faster than under the classical LMPC in the presence and absence of process uncertainty. The results of this chapter originally appeared in.[8]

3.2 Preliminaries

3.2.1 Notation

The transpose of a vector x is represented by the symbol x^T. The Euclidean norm of a vector is denoted by the operator $|\cdot|$. A level set of a sufficiently smooth, positive definite scalar-valued function $V(x)$ is represented by the symbol Ω_ρ ($\Omega_\rho := \{x \in R^n : V(x) \leq \rho\}$). The symbol $S(\Delta)$ denotes the family of piecewise constant, right-continuous functions with period $\Delta \geq 0$. Set subtraction is denoted by the operator '/', that is, $A/B := \{x \in R^n : x \in A, x \notin B\}$.

3.2.2 Class of Systems

Nonlinear process systems are considered with the following state-space description:

$$\dot{x} = f(x,u,w) \tag{3.1}$$

where $x \in \mathbb{R}^n$ is the state of the system, and $u \in \mathbb{R}^m$ and $w \in \mathbb{R}^l$ are the control (manipulated) input vector and the disturbance vector, respectively. The admissible input values are restricted to be in m nonempty convex sets $U_i \subseteq \mathbb{R}$, $i = 1,\ldots,m$, defined as $U_i := \{u_i \in \mathbb{R} : u_i^{\min} \leq u_i \leq u_i^{\max}\}$, where $u_i^{\max}$ and $u_i^{\min}$, $i = 1,\ldots,m$, are the magnitudes of the input constraints. The vector function f is assumed to be a locally Lipschitz vector function of its arguments with $f(0,0,0) = 0$. Further, the

disturbance vector w is assumed to bounded within the set $W := \{w \in \mathbb{R}^l : |w| \leq \theta, \theta > 0\}$ (i.e., $w \in W$).

3.2.3 Lyapunov-Based Controller Assumption

The class of nonlinear systems of Eq. 3.1 is constrained to a class of stabilizable nonlinear systems. Particularly, the existence of a Lyapunov-based controller $h(x) = [h_1(x) \cdots h_m(x)]^T$ which renders the origin of Eq. 3.1 with $w(t) \equiv 0$ (the nominal closed-loop system) asymptotically stable with $h_i(x) \in U_i$, $i = 1, \ldots, m$, inside a given stability region Ω_ρ is assumed. Further, it is assumed that there exist[49,63] a sufficiently smooth Lyapunov function $V(x)$ for the nominal closed-loop system and class $\mathscr{K}$ functions $\alpha_i(\cdot)$, $i = 1, 2, 3, 4$, such that the following inequalities hold:

$$\begin{gathered} \alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|) \\ \frac{\partial V(x)}{\partial x} f(x, h_1(x), \ldots, h_m(x), 0) \leq -\alpha_3(|x|) \\ \left| \frac{\partial V(x)}{\partial x} \right| \leq \alpha_4(|x|) \\ h_i(x) \in U_i,\ i = 1, \ldots, m \end{gathered} \tag{3.2}$$

for all $x \in D \subseteq R^n$ where D is an open neighborhood of the origin. The stability region Ω_ρ of the process of Eq. 3.1 under $h(x)$ (where $\Omega_\rho \subseteq D$) is defined as a level set of the Lyapunov function within which $\dot{V}$ is negative. Designs for stabilizing control laws that account for input constraints for different classes of nonlinear systems have been developed (see, for instance,[27,35,53,59]).

When x is maintained within the compact set Ω_ρ, $u_i \in U_i$, $i = 1, \ldots, m$, and $w \in W$, we have from the continuity of x, the local Lipschitz property of f, and the smoothness of $V(x)$ that there exist positive constants M, L_x, L_w, L'_x and L'_w such that the following inequalities hold:

$$|f(x(t), u(t), w(t))| \leq M \tag{3.3}$$

$$|f(x, u, w) - f(x^*, u, 0)| \leq L_x |x - x^*| + L_w |w| \tag{3.4}$$

$$\left|\frac{\partial V(x)}{\partial x} f(x,u,w) - \frac{\partial V(x^*)}{\partial x} f(x^*,u,0)\right| \leq L'_x |x-x^*| + L'_w |w| \tag{3.5}$$

for all $x, x^* \in \Omega_\rho$, $u_i \in U_i$, $i = 1,\ldots,m$, and $w \in W$.

3.2.4 Lyapunov-Based Model Predictive Control

Lyapunov-based model predictive control (LMPC)[66] is a model predictive control (MPC) strategy that incorporates Lyapunov-based constraints to ensure closed-loop stability of the optimization-based controller. The formulation of the classical LMPC optimization problem is as follows:

$$\min_{u(t)\in S(\Delta)} \int_{t_k}^{t_{k+N}} [\tilde{x}(\tau)^T Q \tilde{x}(\tau) + u(\tau)^T R u(\tau)] d\tau \tag{3.6a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{3.6b}$$

$$u(t) \in U, \ \forall\, t \in [t_k, t_{k+N}) \tag{3.6c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{3.6d}$$

$$V(\tilde{x}(t)) \leq \rho, \ \forall\, t \in [t_k, t_{k+N}) \tag{3.6e}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0) \tag{3.6f}$$

where the decision variable of the optimization problem is the piecewise constant input trajectory $u(t)$. The input constraint of Eq. 3.6c restricts the computed input trajectories to be within the admissible set over the prediction horizon. The nominal model of Eq. 3.1 is incorporated to predict the evolution of the system over the prediction horizon $N\Delta$ (Eq. 3.6b). The notation $\tilde{x}(t)$ and $x(t_k)$ denotes the predicted state trajectory and the state measurement obtained at the sampling time t_k, respectively. The stage cost of the LMPC of Eq. 3.6 is a quadratic function that penalizes the deviations of the state and inputs from their corresponding steady-state values (Eq. 3.6a). The weighting matrices Q and R are tuned to manage the trade-off between the amount of control energy required to move the state to the steady-state and the speed of approach to this steady-

state (even though this trade-off is not transparent). Eqs. 3.6e-3.6f represent the Lyapunov-based constraints where the constraint of Eq. 3.6e maintains the closed-loop state of the process of Eq. 3.1 within the stability region Ω_ρ over the prediction horizon. Finally, the constraint of Eq. 3.6f (contractive constraint) forces the time derivative of the Lyapunov function under the classical LMPC to be less than the time derivative of the Lyapunov function under the explicit stabilizing controller $h(x)$.

3.3 Safety-Based LMPC Design

In this section, an LMPC design is developed that incorporates safety-based constraints (termed safety-LMPC). In the first subsection, the motivation for adding safety-based constraints to the classical LMPC scheme of Eq. 3.6 is provided to form safety-LMPC. In the second and third subsections, the formulations of two proposed safety-LMPC optimization problems are given and the proofs of recursive feasibility and closed-loop stability of one of the safety-LMPC schemes are presented, with discussion of such properties for the other safety-LMPC scheme. In the fourth subsection, the changes required to the proposed safety-LMPC formulations to change the current region of operation to another one around a different steady-state are presented.

3.3.1 Motivation for Safety-Based Constraints

Tracking MPC is widely used in the chemical process industries. The main purpose of tracking MPC is to steer the process to the operating steady-state and maintain process operation at this steady-state. However, in the presence of disturbances, tracking MPC does not guarantee closed-loop stability. Alternatively, the LMPC design of Eq. 3.6 uses the explicit stabilizing controller $h(x)$ to ensure closed-loop stability by decreasing the Lyapunov function value at the beginning of each sampling time. Though LMPC is thus able to guarantee closed-loop stability of the process, always maintaining process operation within Ω_ρ and decreasing the state to a neighborhood of the steady-state, there may be scenarios in which a region within Ω_ρ becomes unsafe to operate within.

In this case, the closed-loop stability properties of LMPC, and the rate at which it drives the state to a neighborhood of the origin through the combination of the contractive constraint and tracking objective function, may not be enough to ensure safe process operation. The rate of approach to the steady-state is lower bounded by the worst-case rate at which $h(x)$ would drive the system to the steady-state when implemented in sample-and-hold, but otherwise is determined by the weighting matrices Q and R and the penalties they place on deviations of the states and inputs from their steady-state values. The only flexibility this classical LMPC formulation offers for changing the rate of approach to the steady-state when process monitoring logic determines that the state needs to move to a smaller level set within the stability region quickly to avoid safety alarms or process shut-down is to adjust Q and R on-line. However, determining appropriate values of Q and R for a desired rate of approach to the safe region of operation is difficult. A method for enhancing the rate of approach to the steady-state when an unsafe situation is detected would allow the process control system to enhance process functional safety.

One method for improving the rate at which the closed-loop state approaches the steady-state is by shrinking the level set used within the LMPC formulation on-line when an unsafe situation is detected. A safe level set of the stability region $\Omega_{\rho_{sp}} \subset \Omega_{\rho}$, termed the safety region, could be identified, outside of which the enhanced rate of decrease would be imposed by shrinking the upper bound on $V(x)$ to force the state to enter smaller level sets at a desired rate. This would have the effect of forcing the state to move toward the origin at a rate potentially faster than that which would be achieved using the quadratic objective and contractive constraint alone. In this chapter, two LMPC schemes are developed termed safety-LMPC 1 and safety-LMPC 2 that can enhance the rate at which the closed-loop state approaches $\Omega_{\rho_{sp}}$.

3.3.2 Safety-LMPC 1 Formulation

Safety-LMPC 1 decreases the upper bound on the Lyapunov function with time to enhance the rate of approach of the closed-loop trajectories to the safety region by imposing a hard constraint within the LMPC scheme that decreases the upper bound on $V(x)$ at a fixed rate. The hard constraint,

which can be utilized in place of Eq. 3.6e, is as follows:

$$V(\tilde{x}(t)) \leq \rho_{sp} + (V(x(t_k)) - \rho_{sp})e^{-a(t-t_k)} \; \forall \; t \in [t_k, t_{k+N}) \tag{3.7}$$

where ρ_{sp} represents the safety set-point. The constant a represents the convergence rate, which can be assigned a value consistent with the rate of approach required to enter the safety region before safety issues occur (which may be a very large value if the required rate of approach is very fast). Based on the value of a, the closed-loop state is required to be within the safety region $\Omega_{\rho_{sp}}$ after a certain number of sampling times to satisfy the constraint. As a result of this constraint, the closed-loop state may enter the safety region more rapidly than under the classical LMPC design of Eq. 3.6. The proposed safety-LMPC 1 guarantees closed-loop stability of the system of Eq. 3.1 in the presence of uncertainty when the safety-LMPC 1 optimization problem is feasible; however, recursive feasibility is not guaranteed because the safety-based constraints may not satisfy the rate that the hard constraint of Eq. 3.7 requires (i.e., the parameter a is significantly large). When the closed-loop state enters ρ_{sp}, the constraint of Eq. 3.7 can be replaced with the constraint of Eq. 3.6e with $\rho = \rho_{sp}$.

Another idea for formulating safety-LMPC 1 with a hard upper bound on the rate of decrease of the Lyapunov function is to utilize a dynamic upper bound $\tilde{\rho}$ on $V(\tilde{x}(t_k))$ that also must meet

Eq. 3.7 as follows:

$$\min_{u(t),K_c(t)\in S(\Delta)} \int_{t_k}^{t_{k+N}} [\tilde{x}(\tau)^T Q\tilde{x}(\tau) + u(\tau)^T Ru(\tau)]d\tau \tag{3.8a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{3.8b}$$

$$u(t) \in U,\ \forall\, t \in [t_k, t_{k+N}) \tag{3.8c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{3.8d}$$

$$K_c(t) \geq 0,\ \forall\, t \in [t_k, t_{k+N}) \tag{3.8e}$$

$$V(\tilde{x}(t)) \leq \tilde{\rho}(t) \leq \rho_{sp} + (V(x(t_k)) - \rho_{sp})e^{-a(t-t_k)},\ \forall t \in [t_k, t_{k+N}) \tag{3.8f}$$

$$\frac{d\tilde{\rho}}{dt} = K_c(t)(\rho_{sp} - \tilde{\rho}(t)) \tag{3.8g}$$

$$\tilde{\rho}(t_k) = V(x(t_k)), \quad \text{if } x(t_k) \notin \Omega_{\rho_{sp}}$$

$$\tilde{\rho}(t_k) = \rho_{sp}, \quad \text{if } x(t_k) \in \Omega_{\rho_{sp}} \tag{3.8h}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0) \tag{3.8i}$$

where the notation follows that in Eq. 3.6. In addition to the manipulated input trajectory $u(t)$, the gain $K_c(t)$ is another decision variable that is restricted to take nonnegative values over the prediction horizon $N\Delta$ (Eq. 3.8e). The performance index of the safety-LMPC 1 is the objective function of the classical LMPC of Eq. 3.6.

Eqs. 3.8e-3.8h represent the safety-based constraints. The contractive constraint (Eq. 3.8i) ensures that the closed-loop state enters $\Omega_{\rho_{sp}}$ in finite time by utilizing the explicit stabilizing controller $h(x)$ to compute control actions that decrease the value of the Lyapunov function at least as much as the decrease given by $h(x)$. Though the constraint of Eq. 3.8i ensures that the closed-loop state of the process of Eq. 3.1 converges to the safety region $\Omega_{\rho_{sp}}$ at a rate that is at least as fast as that which the explicit stabilizing controller $h(x)$ would offer in a worst case (it may be faster depending on Q and R), the role of the safety-based constraints is to enhance the rate of decrease of the state until it enters $\Omega_{\rho_{sp}}$ in the required number of sampling times that the hard constraint

of Eq. 3.8f imposes, and then to resume the normal rate of approach to the steady-state using the classical LMPC scheme. This allows the original tuning of the objective function with respect to Q and R to retain its significance once the state is within a safe region of operation, and also allows for the rate of decrease toward the safety region to potentially be faster than it would be under the classical LMPC design alone. Specifically, the upper bound (Eq. 3.7) in the constraint of Eq. 3.8f enforces a fast rate of approach of the state to $\Omega_{\rho_{sp}}$ by causing the optimization problem to choose a K_c that will decrease the upper bound $\tilde{\rho}(t)$ on the Lyapunov function value of the predicted state as quickly as the rate of approach (parametrized by a) required to enter the safety region. This has the potential to decrease the level set of the predicted Lyapunov function value $V(\tilde{x}(t))$ over the prediction horizon more significantly than under the classical LMPC design alone, causing the closed-loop state to move more quickly toward the safety region $\Omega_{\rho_{sp}}$. The rate at which $\tilde{\rho}$ decreases is governed by the magnitude of the decision variable $K_c(t)$ in the first-order ordinary differential equation of Eq. 3.8g. Moreover, the predicted state trajectory $\tilde{x}(t)$ is maintained within the predicted level set $\Omega_{\tilde{\rho}(t)}$ over the prediction horizon by the constraint of Eq. 3.8f, so that the predicted state cannot leave $\Omega_{\tilde{\rho}}$ in a given prediction horizon once it enters it. To ensure that the classical LMPC design of Eq. 3.6 can be recovered when the optimization problem of Eq. 3.8 causes the state to enter $\Omega_{\rho_{sp}}$, the safety-LMPC utilizes state feedback to set the initial condition of the constraint of Eq. 3.8g to the value of the Lyapunov function at the current state when the state measurement is outside the safety region $\Omega_{\rho_{sp}}$, or to the safety set-point ρ_{sp} if the current state enters the safety region (i.e., $x(t_k) \in \Omega_{\rho_{sp}}$) (Eq. 3.8h). Thus, when $x(t_k)$ enters the safety region, the classical LMPC design is recovered because the constraint of Eq. 3.8g will be set to zero.

The constraint of Eq. 3.8f may be more likely to become infeasible than the constraint of Eq. 3.7 because it requires that the dynamics of both the nominal process (Eq. 3.8b) and the dynamics of $\tilde{\rho}$ (Eq. 3.8g) cause Eq. 3.8f to be met. However, the LMPC of Eq. 3.8 has the advantage of being more readily transformed to the soft constraint formulation that will be developed in the next subsection than does the LMPC formulation of Eq. 3.6 with Eq. 3.7 (and hence further discussion on this point will be deferred to that subsection). Despite the possible infeasibility of the safety-

LMPC 1 formulation, the safety-based constraint allows it to require an explicit rate of decrease of the Lyapunov function value until the closed-loop state enters the safety region, which would be difficult to achieve by tuning Q and R if the safety-based constraints were not utilized.

Remark 3.1 *The proposed safety-LMPC design does not study the process complexity itself (the nonlinear, coupled nature of the process dynamics is considered to be an innate aspect of the physics and chemistry of the process), rather this chapter is focused on the problem of the complexity (difficulty) of ensuring safe operation of nonlinear, highly coupled processes. The new solution proposed by this chapter is a control design that explicitly incorporates safety-based state constraints that guarantee recursive feasibility and closed-loop stability of a process under the controller, and also guarantee that the closed-loop process can be driven into a safe region of operation in finite time, under certain conditions. The new controller design proposed below can handle the difficulty associated with the conventional tracking MPC formulation in which it is not obvious how to adjust the matrices Q and R on-line so that the rate of approach to the steady-state when process monitoring logic determines that the state needs to move faster to a safe region of operation is enhanced. However, the proposed safety-LMPC design enhances the rate of approach to the steady-state by incorporating safety-based constraints and a safety penalty term that can shrink the level set used within the MPC formulation on-line. Subsequently, the process state will move toward the safe region of operation at a rate potentially faster than that which would be achieved using the quadratic objective function of the conventional tracking-MPC. Thus, the proposed formulation avoids the difficulty of tuning the Q and R matrices due to safety considerations and can still achieve the goal of driving the closed-loop state to a region of operation closer to the steady-state at a faster rate than would otherwise be attained with the Q and R matrices unchanged.*

Remark 3.2 *It is noted that the safety-based constraints do not guarantee a decrease in the Lyapunov function value of the closed-loop state at the rate given by Eq. 3.8g because the dynamics of $V(x)$ are not those in Eq. 3.8g and furthermore process disturbances will cause the value of $V(x)$ along the actual closed-loop state trajectory to differ from the predicted upper bound in Eq. 3.8.*

However, when $K_c(t)$ and $u(t)$ decrease $\tilde{\rho}(t)$ significantly, it is possible that the actual process state will be decreased significantly for that same value of the input, which may cause the closed-loop state under Eq. 3.8 to be driven into $\Omega_{\rho_{sp}}$ more quickly than it would be under Eq. 3.6.

Remark 3.3 *Though $K_c(t)$ is piecewise constant with period Δ in Eq. 3.8, it is not a physical quantity and thus could be piecewise constant with a different period if desired.*

Remark 3.4 *Though it is possible to continue to enforce the enhanced rate of decrease to the steady-state from Eq. 3.7 or 3.8f even after the closed-loop state enters $\Omega_{\rho_{sp}}$, this would not in general be desirable because the weighting matrices Q and R are typically chosen to allow a trade-off between the rate of approach to the steady-state and the use of the inputs. If the safety-based constraints of the safety-LMPC were always active and drove the state quickly toward the origin, Q and R would lose their value as tuning parameters because the effect would be like having a large Q.*

Remark 3.5 *An alternative upper bound in Eqs. 3.7 and 3.8f is $(\rho_{sp}+(V(x(t_{saf}))-\rho_{sp})e^{-a(t-t_{saf})})$, where t_{saf} corresponds to the time at which process monitoring logic requests that the closed-loop state begin to move toward the safety region. This upper bound ensures that the only change in the value of the upper bound is due to t increasing, whereas the upper bound in Eqs. 3.7 and 3.8f changes not only due to t changing, but also due to changes in $V(x(t_k))$ and t_k. Thus, the requested rate of decrease toward the safety region corresponding to the former upper bound may be more easily understood a priori using the decaying exponential, whereas it is more difficult to determine the rate of decrease throughout time with the latter upper bound because at any given sampling period it depends on the process state measurement $x(t_k)$, which is affected by prior chosen control actions and process disturbances that cannot be known a priori.*

3.3.3 Safety-LMPC 2 Formulation

The second safety-LMPC formulation that is proposed in this chapter is a modification of the formulation of safety-LMPC 1 such that the resulting controller, termed safety-LMPC 2, forces the

closed-loop state to go to $\Omega_{\rho_{sp}}$ while recursive feasibility and closed-loop stability of the process of Eq. 3.1 under safety-LMPC 2 are guaranteed. The mathematical formulation of safety-LMPC 2 for the process of Eq. 3.1 is as follows:

$$\min_{u(t),K_c(t)\in S(\Delta)} \int_{t_k}^{t_{k+N}} [\tilde{x}(\tau)^T Q\tilde{x}(\tau) + u(\tau)^T Ru(\tau) + \phi(\rho_{sp} - \tilde{\rho}(\tau))]d\tau \tag{3.9a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{3.9b}$$

$$u(t) \in U, \ \forall\, t \in [t_k, t_{k+N}) \tag{3.9c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{3.9d}$$

$$K_c(t) \geq 0, \ \forall\, t \in [t_k, t_{k+N}) \tag{3.9e}$$

$$V(\tilde{x}(t)) \leq \tilde{\rho}(t), \ \forall\, t \in [t_k, t_{k+N}) \tag{3.9f}$$

$$\frac{d\tilde{\rho}}{dt} = K_c(t)(\rho_{sp} - \tilde{\rho}(t)) \tag{3.9g}$$

$$\tilde{\rho}(t_k) = V(x(t_k)), \quad \text{if } x(t_k) \notin \Omega_{\rho_{sp}}$$

$$\tilde{\rho}(t_k) = \rho_{sp}, \quad \text{if } x(t_k) \in \Omega_{\rho_{sp}} \tag{3.9h}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0) \tag{3.9i}$$

where the notation follows that in Eq. 3.8. The performance index of the safety-LMPC 2 formulation includes the objective function of the classical LMPC of Eq. 3.6 and a safety penalty term as in Chapter 2. The safety penalty term $\phi(\rho_{sp} - \tilde{\rho}(t))$ penalizes the deviation of the upper bound of the Lyapunov function value $\tilde{\rho}(t)$ from the safety set-point ρ_{sp} over the prediction horizon. Specifically, the penalty term in the objective can be appropriately weighted to enforce a fast rate of approach of the state to $\Omega_{\rho_{sp}}$ by causing the optimization problem to choose a K_c that will decrease the upper bound $\tilde{\rho}(t)$ on the Lyapunov function value of the predicted state rapidly. This has the potential to decrease the value of the Lyapunov function along the predicted closed-loop state trajectories ($V(\tilde{x}(t))$) over the prediction horizon more significantly than under the classical

LMPC design alone, causing the closed-loop state to move more quickly toward the safety region $\Omega_{\rho_{sp}}$. However, the rate of decrease to the safety region does not necessarily meet the convergence rate required by Eq. 3.7 because safety-LMPC 2 enforces the hard constraint of Eq. 3.7 as a soft constraint through a penalty term in the objective function to drive the closed-loop state to $\Omega_{\rho_{sp}}$ while feasibility of the optimization problem is guaranteed for all times.

It was noted in the prior section that the benefits of the dynamic upper bound $\tilde{\rho}$ utilized within the safety-LMPC 1 formulation in Eq. 3.8 (as opposed to the formulation of Eq. 3.6 with Eq. 3.7) would be more clear after the formulation of safety-LMPC 2 had been introduced, and they will now be discussed. Specifically, the formulation of Eq. 3.8 clarifies the relationship between the desired rate of approach to the safety region as parametrized by a and the gain K_c calculated by the LMPC (i.e., a specific gain K_c must be chosen in any given sampling period if the rate of approach parameterized by a is to be met in Eq. 3.8f). This is helpful in understanding how the rate of approach to the steady-state is embedded within the soft constraint formulation of Eq. 3.9 through the gain K_c. Furthermore, the closeness of the formulations of Eqs. 3.8 and 3.9 is beneficial because it provides a strategic set-up for, for example, employing logic that enforces a specific rate of decrease through Eq. 3.8 when that optimization problem is feasible but then switches to the soft constraint formulation of Eq. 3.9 with minimal adjustment of the optimization problem when Eq. 3.8 becomes infeasible (i.e., only a penalty on the objective function and the removal of the upper bound on $\tilde{\rho}$ in Eq. 3.8f need to be implemented when infeasibility occurs to obtain a control action that can guarantee closed-loop stability and controller feasibility; the transition to the modified optimization problem is not as smooth with the formulation of Eq. 3.6 with Eq. 3.7, for which new constraints and optimization variables would need to be added to the optimization problem to enable the transition).

Safety-LMPC 2 provides two primary benefits in terms of enforcing the rate of approach of the closed-loop state to the safety region that cannot easily be obtained by tuning Q and R in an LMPC formulation without safety-based constraints. Firstly, safety-LMPC 2 may aid as noted in the previous paragraph in developing a controller design that can easily transition between the

LMPC formulation of Eq. 3.8 and that of Eq. 3.9 whenever Eq. 3.8 becomes infeasible to encourage the closed-loop state to meet the explicit rate of approach to the closed-loop state (that could not easily be determined by adjusting Q and R) that is enforced by Eq. 3.8f as closely as possible. Furthermore, even if safety-LMPC 2 is utilized on its own (i.e., not with Eq. 3.8), safety-LMPC 2 still allows for one parameter (the weighting on the penalty on $(\rho_{sp} - \tilde{\rho})$ in the objective function) to be adjusted to alter the rate of approach to the safety region as desired. When it is unclear how large this weight should be for a desired rate of approach, it can be adjusted based on process data. Specifically, the rate at which the closed-loop state moves toward the safety region can be evaluated based on measurements of the process state between sampling times. Then, based on whether this rate is appropriate for the safety concerns at hand, the weight can be increased (to drive the process state toward the safety region more quickly) or decreased (if the rate is faster than required and is using more control action than desired). The relative weighting on the safety penalty term compared to the quadratic terms in the objective function may depend on the process dynamics and the length of time remaining until it is desired that the state be within the safety region. This allows the difficult problem of adjusting Q and R at the same time (which involves not just tuning two different quantities with respect to one another, but also all of the individual values within both matrices) to achieve a desired rate of approach to the safety region to be simplified to the problem of adjusting only one parameter, the weighting on the penalty term.

Remark 3.6 *The main objective of this chapter is to enhance the safety performance of the conventional tracking MPC by imposing safety-based constraints and Lyapunov-based constraints into the MPC so that the process state variables can be driven to the safety region at a faster rate than the conventional tracking MPC would offer. The safety region is defined as a level set of the stability region where the process state variables stay within a range that prevents triggering of safety alarms. Similar to the conventional tracking MPC, the proposed safety-LMPC can be applied to nonlinear systems that do not obey the superposition principle which defines linear systems. Our scope includes the nonlinear processes and it also includes a number of assumptions regarding process safety, such as that there are no actions from the safety system interfering with the actions*

of the control system, that the region of safe operation can be pre-determined on-line as a level set. Also, this chapter considers controlling a nonlinear process (in terms of its dynamics, the underlying differential equations describing the physical-chemical phenomena are nonlinear ordinary differential equations) with an MPC that includes safety constraints. MPC's should be equipped with a sufficiently accurate process model to provide accurate state predictions; in this chapter, it is considered that the MPC includes a nonlinear process model to make state predictions. It is in that sense that the MPC incorporates nonlinearity (i.e., the MPC determines optimal control actions to apply based on how it predicts these control actions will affect the state of a nonlinear process throughout the prediction horizon, and also the control actions are applied to a nonlinear process). Therefore, LMPC is a nonlinear controller as it has constraints and uses a nonlinear model to compute control actions that regulate the nonlinear process state - LMPC is not a linear controller.

Feasibility and Stability Analysis of Safety-LMPC 2

In this subsection, sufficient conditions are presented such that the state of the closed-loop system of Eq. 3.1 under the safety-LMPC 2 design is guaranteed to enter the safety region $\Omega_{\rho_{sp}}$ in finite time and reside within the safety region $\Omega_{\rho_{sp}}$ thereafter. Moreover, it is proved that the closed-loop state is guaranteed to be ultimately bounded within a compact set containing the origin. Because safety-LMPC 1 is not guaranteed to be recursively feasible but safety-LMPC 2 is, the feasibility and stability analysis is only presented for safety-LMPC 2, though the closed-loop stability results also hold for both safety-LMPC 1 formulations (Eq. 3.6 with Eq. 3.7 and Eq. 3.8) when those formulations are recursively feasible. The following theorem provides sufficient conditions that prove practical stability of the system of Eq. 3.1 under the proposed safety-LMPC 2 design.

Theorem 3.1 *Consider the system of Eq. 3.1 in closed-loop under the safety-LMPC 2 design of Eq. 3.9 based on a controller $h(x)$ that satisfies the conditions of Eq. 3.2. Let $\varepsilon_w > 0$, $\Delta > 0$,*

$\rho > \rho_{sp} > \rho_s > 0$ *satisfy*

$$-\alpha_3(\alpha_2^{-1}(\rho_s)) + L_x' M\Delta + L_w'\theta \leq -\varepsilon_w/\Delta. \tag{3.10}$$

If $x(t_0) \in \Omega_\rho$, $\rho_{\min} \leq \rho$ *and* $N \geq 1$ *where*

$$\rho_{\min} = \max\{V(x(t+\Delta)) : V(x(t)) \leq \rho_s\}, \tag{3.11}$$

then the closed-loop state $x(t)$ *of Eq. 3.1 is guaranteed to enter the safety region* $\Omega_{\rho_{sp}}$ *in finite time and then reside there, and also the state* $x(t)$ *of the closed-loop system is ultimately bounded in* $\Omega_{\rho_{\min}}$.

Proof 3.1 *The proof consists of two parts. The first part includes the proof of the feasibility of the safety-LMPC 2 optimization problem for all states* $x(t) \in \Omega_\rho$. *The second part includes the proof of the two results of Theorem 3.1.*

Part 1: The proposed safety-LMPC 2 of Eq. 3.9 is always a feasible optimization problem. The feasibility of the safety-LMPC 2 formulation is guaranteed because the following solution is always feasible:

$$\begin{aligned} &K_c(t) = 0,\ \forall\, t \in [t_k, t_{k+N}), \\ &u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1}) \\ &\text{with } n = k, \ldots, N+k-1, \end{aligned} \tag{3.12}$$

The proof of feasibility of the solution of Eq. 3.12 is given in four steps: 1) the gain $K_c(t) = 0, \forall\, t \in [t_k, t_{k+N})$ *is feasible since it satisfies Eq. 3.9e over the prediction horizon 2) when* $K_c(t) = 0$ *throughout the prediction horizon, then by Eq. 3.9g,* $\tilde{\rho}(t)$ *will be equal to its initial value from Eq. 3.9h throughout the prediction horizon, and hence the upper bound on the Lyapunov function in Eq. 3.9f will remain constant (i.e., either* $\tilde{\rho}(t_k) = V(x(t_k)) \Rightarrow V(\tilde{x}(t)) \leq V(x(t_k)), \forall\, t \in [t_k, t_{k+N}), \text{if } x(t_k) \notin \Omega_{\rho_{sp}}$ *or* $\tilde{\rho}(t_k) = \rho_{sp} \Rightarrow V(\tilde{x}(t)) \leq \rho_{sp}, \forall\, t \in [t_k, t_{k+N}), \text{if } x(t_k) \in \Omega_{\rho_{sp}}$*) 3) when* $\tilde{\rho}$

is constant, the feasibility of $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$, *with* $n = k, \ldots, N+k-1$, *is guaranteed because it satisfies the input constraint of Eq. 3.9c and also, because of the closed-loop stability property of the Lyapunov-based controller* $h(x)$,[72] *it satisfies the constraint of Eq. 3.9f, 4) finally,* $u(t) = h(\tilde{x}(t_n)), \forall\, t \in [t_n, t_{n+1})$, *with* $n = k, \ldots, N+k-1$, *satisfies the contractive constraint of Eq. 3.9i making it a feasible input trajectory for the safety-LMPC 2 design. Therefore, the solution of Eq. 3.12 is a feasible solution, and recursive feasibility of the safety-LMPC 2 follows if the closed-loop state trajectory is maintained within* Ω_ρ.

Part 2: In this part, it is proved that if the closed-loop state $x(t_k)$ *is initialized within the stability region, but outside the safety region (i.e.,* $x(t_k) \in \Omega_\rho / \Omega_{\rho_{sp}}$), *then within finite time the closed-loop state will enter the safety region* $\Omega_{\rho_{sp}}$, *and also will be ultimately bounded in a small region containing the origin* $\Omega_{\rho_{\min}}$.

If $x(t_k) \in \Omega_\rho / \Omega_{\rho_s}$, *then due to the contractive constraint of Eq. 3.9i in the safety-LMPC 2 formulation of Eq. 3.9, the Lyapunov function of the closed-loop state will decrease for the first sampling period in the prediction horizon by at least the rate given by the explicit stabilizing controller* $h(x)$. *Owing to the closed-loop stability property of the explicit controller* $h(x)$,[72] *the Lyapunov function value of the closed-loop state under the safety-LMPC design will decrease in the next sampling period (i.e.,* $V(x(t)) \leq V(x(t_k)); \forall\, t \in [t_k, t_{k+1}]$, *which is derived in.*[43] *Thus, if* $x(t_k) \in \Omega_\rho / \Omega_{\rho_s}$ *then* $V(x(t_{k+1})) < V(x(t_k))$ *and in finite time, the closed-loop state converges to* Ω_{ρ_s} *(i.e.,* $x(t_{k+j}) \in \Omega_{\rho_s}$ *where* j *is a finite positive integer). By the definitions of* ρ_s *and* $\rho_{\min}$ *in Theorem 3.1, once the closed-loop state converges to* $\Omega_{\rho_s} \subseteq \Omega_{\rho_{\min}}$, *it remains inside* $\Omega_{\rho_{\min}}$ *for all times. This proves the second result of Theorem 3.1 which is the ultimate boundedness of the closed-loop state in* $\Omega_{\rho_{\min}}$. *However, the first result of Theorem 3.1 which is that the closed-loop state converges to the safety region* $\Omega_{\rho_{sp}}$ *in finite time and then resides there is a result of the previous proof due to the assumption that* $\rho_{sp} > \rho_s$ *which is stated in Theorem 3.1.*

3.3.4 Safety Region Changes

The safety-LMPC formulations of Eq. 3.6 with 3.7 and of Eqs. 3.8-3.9 assume that $\Omega_{\rho_{sp}}$ is a subset of Ω_ρ. However, there may be scenarios in which the safety logic unit indicates that regions within the current stability region Ω_ρ are no longer safe to operate within, but that another safety region that is a subset of a different stability region is appropriate. Therefore, it is necessary to modify the safety-LMPC during the transition between the stability regions in a manner that allows the region of operation to shift. The manner in which the safety-based LMPC formulation should be modified depends on the configuration of the old stability and safety regions (Ω_{ρ_1} and $\Omega_{\rho_{sp1}}$ respectively) with respect to the newly requested stability and safety regions (Ω_{ρ_2} and $\Omega_{\rho_{sp2}}$ respectively). This will be illustrated by presenting two example configurations in the context of the safety-LMPC 2 of Eq. 3.9, though the closed-loop stability results noted will also hold for the safety-LMPC 1 formulations of Eq. 3.6 with 3.7 and of Eq. 3.8 when those LMPC's are feasible.

Figure 3.1 shows one possible configuration (Configuration 1) of the two different safe regions of operation $\Omega_{\rho_{sp1}}$ and $\Omega_{\rho_{sp2}}$. For this configuration, the safety-LMPC 2 of Eq. 3.9 will be applied with $\rho_{sp} = \rho_{sp1}$ until the closed-loop state enters $\Omega_{\rho_{sp1}}$. At the switching time t_s, the safety logic unit determines that $\Omega_{\rho_{sp2}}$ is the new safe region of operation, which is a subset of the stability region Ω_{ρ_2}. Therefore, at this time ρ_{sp} in the formulation of Eq. 3.9 will be changed to ρ_{sp2} (the quadratic terms in the objective function, nominal process model, and Lyapunov function will also be reformulated to have their origins at the new steady-state). Because the first safety region $\Omega_{\rho_{sp1}}$ is contained within the stability region Ω_{ρ_2} and the safety-LMPC 2 of Eq. 3.9 with $\rho_{sp} = \rho_{sp2}$ drives the closed-loop state into $\Omega_{\rho_{sp2}}$ from any initial condition in Ω_{ρ_2}, the safety-LMPC 2 of Eq. 3.9 is feasible after t_s and guarantees that the closed-loop state will be driven from $\Omega_{\rho_{sp1}}$ into $\Omega_{\rho_{sp2}}$ in finite time.

Figure 3.2 shows a second possible configuration (Configuration 2) of Ω_{ρ_1}, $\Omega_{\rho_{sp1}}$, Ω_{ρ_2}, and $\Omega_{\rho_{sp2}}$. In this case, $\Omega_{\rho_{sp1}}$ is not fully within the stability region Ω_{ρ_2}. To drive the closed-loop state from any initial condition within $\Omega_{\rho_{sp1}}$ into $\Omega_{\rho_{sp2}}$ after t_s, one method is to remove the constraints of Eqs. 3.9e-3.9i and the safety penalty term in the objective function (formulated with $\rho_{sp} = \rho_{sp1}$)

from Eq. 3.9 at t_s, and to instead utilize a terminal region constraint (e.g., $\tilde{x}(t_{s+\bar{N}}) \in \Omega_{\rho_2}$) with a sufficiently long prediction horizon $\bar{N}$ to drive the closed-loop state into Ω_{ρ_2} by the end of the prediction horizon. However, due to the hard terminal constraint, feasibility of this optimization problem is not guaranteed. The formulation of the proposed safety-LMPC for the process of Eq. 3.1 to be used during the transition from $\Omega_{\rho_{sp1}}$ to Ω_{ρ_2} is as follows:

$$\min_{u(t)\in S(\Delta)} \int_{t_k}^{t_{k+\bar{N}}} [\tilde{x}(\tau)^T Q \tilde{x}(\tau) + u(\tau)^T R u(\tau)] d\tau \tag{3.13a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{3.13b}$$

$$u(t) \in U, \ \forall \ t \in [t_k, t_{k+\bar{N}}) \tag{3.13c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{3.13d}$$

$$V_2(\tilde{x}(t_{s+\bar{N}}) \leq \rho_2, \ \forall \ t \in [t_{s+\bar{N}}, t_{k+\bar{N}}] \tag{3.13e}$$

$$V_1(\tilde{x}(t)) \leq \rho_1, \ \forall \ t \in [t_k, t_{s+\bar{N}}) \tag{3.13f}$$

where the objective function, nominal process model, and Lyapunov function V_1 for the old steady-state have their minimums at the original steady-state, but the Lyapunov function V_2 for the new steady-state has its origin at the new steady-state. In the transitioning period, the terminal region constraint of Eq. 3.13e will be activated with a sufficiently long prediction horizon $\bar{N}$ to force the closed-loop state to be within the second stability region Ω_{ρ_2} at the end of the prediction horizon $t_{s+\bar{N}}$. If the closed-loop state is outside the second stability region Ω_{ρ_2} at the switching time t_s, feasibility of the proposed controller of Eq. 3.13 is not guaranteed. The Lyapunov-based constraint of Eq. 3.13f is imposed to guarantee that the closed-loop state chooses a path that does not go outside the first stability region Ω_{ρ_1} to maintain closed-loop stability of the process in the transitioning period. In other words, the closed-loop state will be driven to the intersection between the two stability regions Ω_{ρ_1} and Ω_{ρ_2}. After that, the safety-LMPC of Eq. 3.8 will be applied with $\rho_{sp} = \rho_{sp2}$ and the objective function, Lyapunov function, and nominal process model with their origins at the new steady-state to drive the closed-loop state into the safety region $\Omega_{\rho_{sp2}}$.

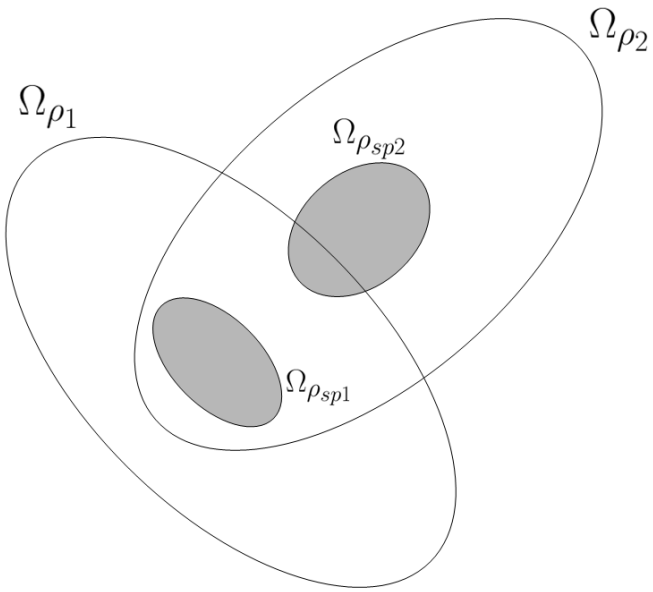

Figure 3.1: Configuration 1 for switching between two different safe regions of operation.

An alternative method for attempting the safety region transition is to remove the contractive constraint from Eq. 3.9 at t_s and to add a soft constraint (e.g., a penalty on $(V(\tilde{x}(t)) - \rho_2)$) in the objective function to encourage the LMPC to compute control actions that drive the closed-loop state into Ω_{ρ_2}. Though this approach would always be feasible, there is still no guarantee that the state will be driven into Ω_{ρ_2}. However, once the state enters Ω_{ρ_2}, the LMPC problem of Eq. 3.9 with $\rho_{sp} = \rho_{sp2}$ and the appropriate modifications to the objective function, f, and V could be used to drive the state into $\Omega_{\rho_{sp2}}$. These two example configurations show that the manner in which Ω_{ρ_1}, $\Omega_{\rho_{sp1}}$, Ω_{ρ_2}, and $\Omega_{\rho_{sp2}}$ are related to each other (e.g., how they intersect) determines how the safety-LMPC 2 of Eq. 3.9 should be modified at t_s until the state enters Ω_{ρ_2} to drive the state into the new stability region, and also whether this can be achieved while guaranteeing closed-loop stability and feasibility.

3.4 Application to a Chemical Process Example

To illustrate the safety advantage of the safety-LMPC paradigm over the classical LMPC, a chemical process example is considered which is a well-mixed, non-isothermal continuous stirred tank

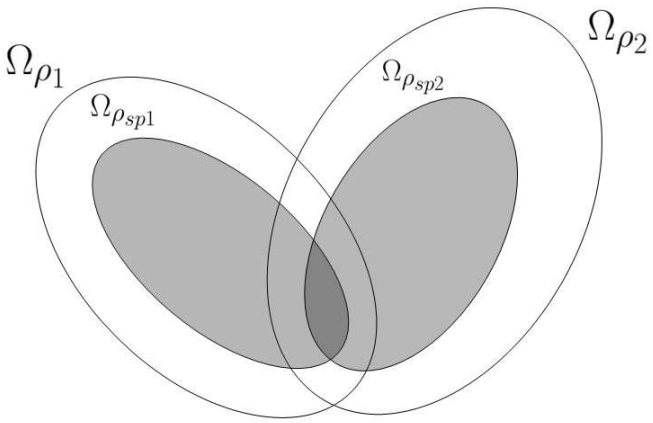

Figure 3.2: Configuration 2 for switching between two different safe regions of operation.

Table 3.1: Parameter values

$T_0 = 300$	K	$F = 5$	$\frac{m^3}{hr}$
$V = 1.0$	m^3	$E = 5 \times 10^4$	$\frac{kJ}{kmol}$
$k_0 = 8.46 \times 10^6$	$\frac{m^3}{kmol hr}$	$\Delta H = -1.15 \times 10^4$	$\frac{kJ}{kmol}$
$C_p = 0.231$	$\frac{kJ}{kgK}$	$R = 8.314$	$\frac{kJ}{kmolK}$
$\rho_L = 1000$	$\frac{kg}{m^3}$	$C_{As} = 2$	$\frac{kmol}{m^3}$
$T_s = 400$	K	$C_{A0s} = 4$	$\frac{kmol}{m^3}$
$Q_s = 0$	$\frac{kJ}{hr}$		

reactor (CSTR). The reaction transforms a reactant A to a product B through an irreversible, exothermic second-order reaction $A \rightarrow B$. The feed of the CSTR consists of pure A and the inlet concentration of A is C_{A0}. The inlet temperature and feed volumetric flow rate of the reactor are T_0 and F, respectively. By applying material and energy balances under standard modeling assumptions, the concentration of A (C_A) and temperature T are modeled as follows:

$$\frac{dC_A}{dt} = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{RT}} C_A^2 \tag{3.14a}$$

$$\frac{dT}{dt} = \frac{F}{V}(T_0 - T) + \frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{RT}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{3.14b}$$

The notation ΔH, k_0, E, and R represent the enthalpy of reaction, pre-exponential constant, activation energy, and ideal gas constant, respectively. The reactor volume V, heat capacity C_p, and

fluid density ρ_L within the reactor are assumed constant. Table 3.1 shows the values of the process parameters used in the simulations. The dynamic model of Eq. 3.14 is numerically simulated by using the explicit Euler method with an integration time step of $h_c = 10^{-5}\ hr$.

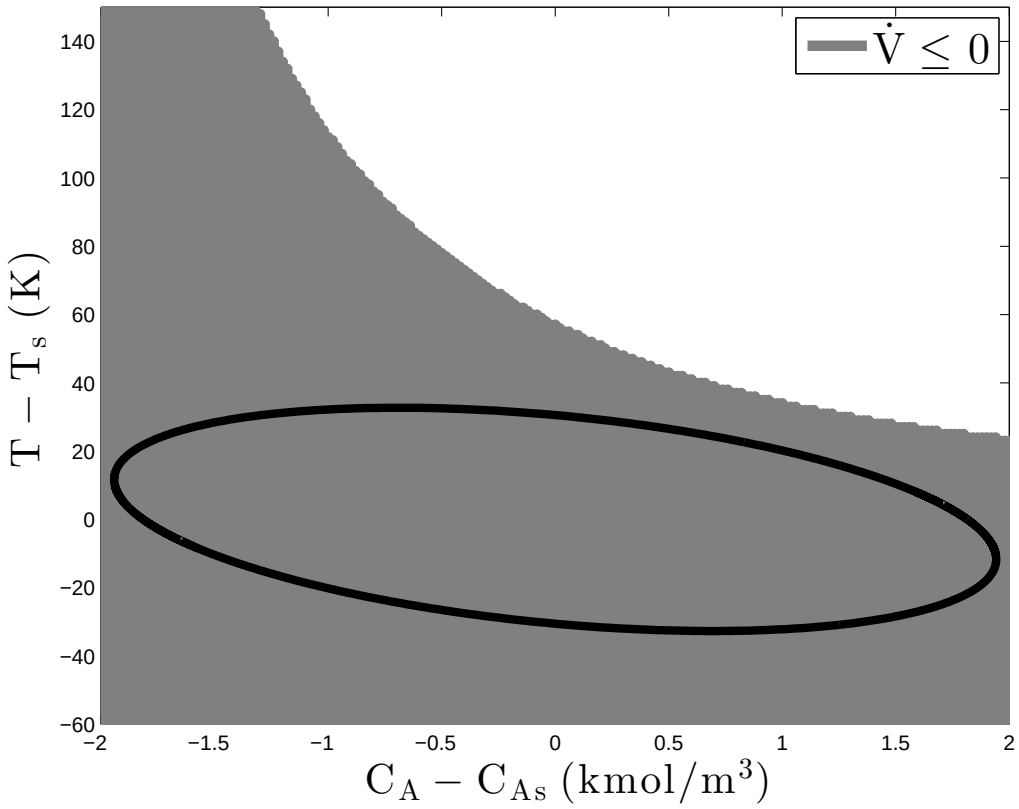

Figure 3.3: The stability region (black ellipse) for the closed-loop CSTR under the explicit stabilizing controller $h(x)$ of Eq. 5.28.

The two states of the CSTR are C_A and T, and the two manipulated inputs are C_{A0} and Q. In this simulation, the safety-LMPC 2 of Eq. 3.9 is applied to the closed-loop CSTR due to its guaranteed closed-loop stability and recursive feasibility properties in the presence of uncertainty. The process of Eq. 3.14 is operated at an unstable steady-state $[C_{As}\ T_s] = [2\ \frac{kmol}{m^3}\ 400\ K]$ with associated steady-state input values $[C_{A0s}\ Q_s] = [4\ \frac{kmol}{m^3}\ 0\ \frac{kJ}{hr}]$ to demonstrate the ability of the safety-LMPC 2 to enhance process functional safety even around open-loop unstable operating points. The nonlinear

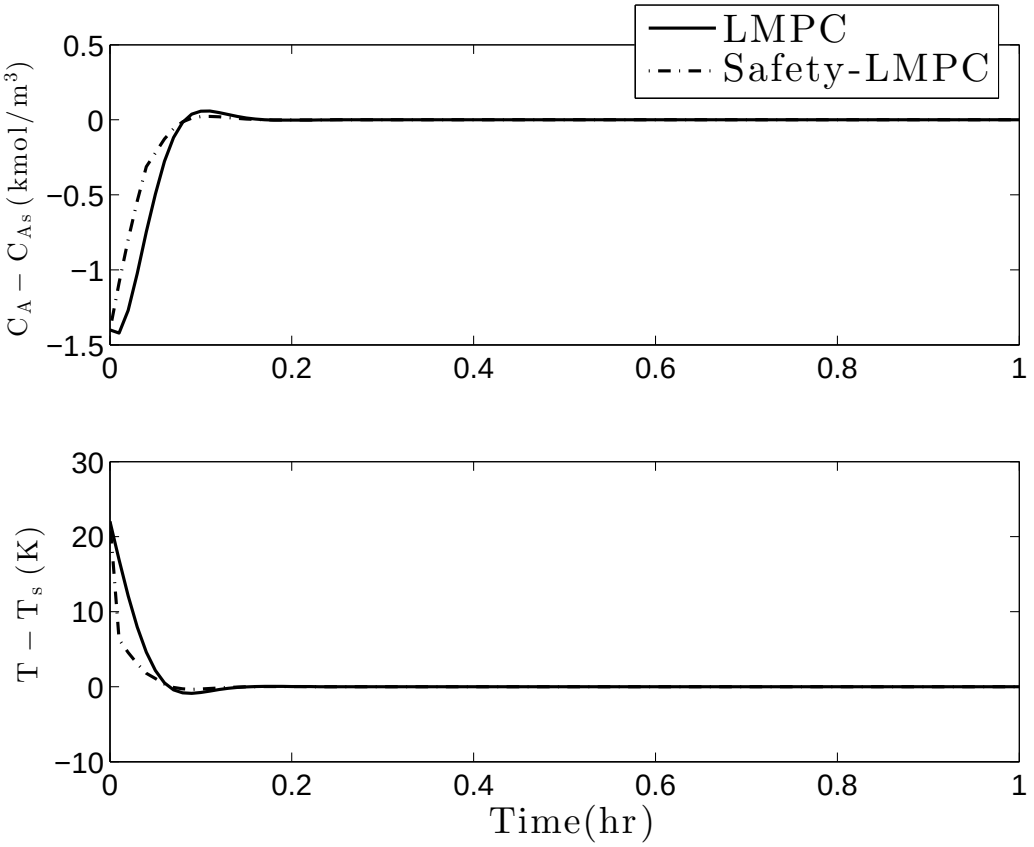

Figure 3.4: The state profiles for the closed-loop CSTR under the classical LMPC design of Eq. 3.6 and under the safety-LMPC design of Eq. 3.9 for the initial condition $x_{int} = [-1.42192\ \frac{kmol}{m^3}\ 22\ K]$ without process disturbances.

process of Eq. 3.14 can be formulated as the following class of nonlinear systems

$$\dot{x}(t) = \tilde{f}(x(t)) + g_1(x(t))u_1(t) + g_2(x(t))u_2(t) \tag{3.15}$$

where $x(t)$ and $u(t)$ denote the state and the manipulated inputs of the CSTR in deviation variable form (i.e., $x^T = [C_A - C_{As}\ T - T_s]$ is the state vector and $u^T = [C_{A0} - C_{A0s}\ Q - Q_s]$ is the manipulated input vector), $\tilde{f}^T = [\tilde{f}_1\ \tilde{f}_2]$ is a vector containing the terms in the CSTR model that do not include u_1 or u_2, and $g_i^T = [g_{i1}\ g_{i2}]$ $(i = 1,2)$ is a vector containing the terms in the CSTR model that multiply u_1 (for $i = 1$) or u_2 (for $i = 2$). The magnitudes of the manipulated inputs are bounded as follows: $|u_1| \leq 3.5\ \frac{kmol}{m^3}$ and $|u_2| \leq 5 \times 10^5\ \frac{kJ}{hr}$.

The safety-LMPC 2 for the process of Eq. 3.14 is designed to compute feasible control actions

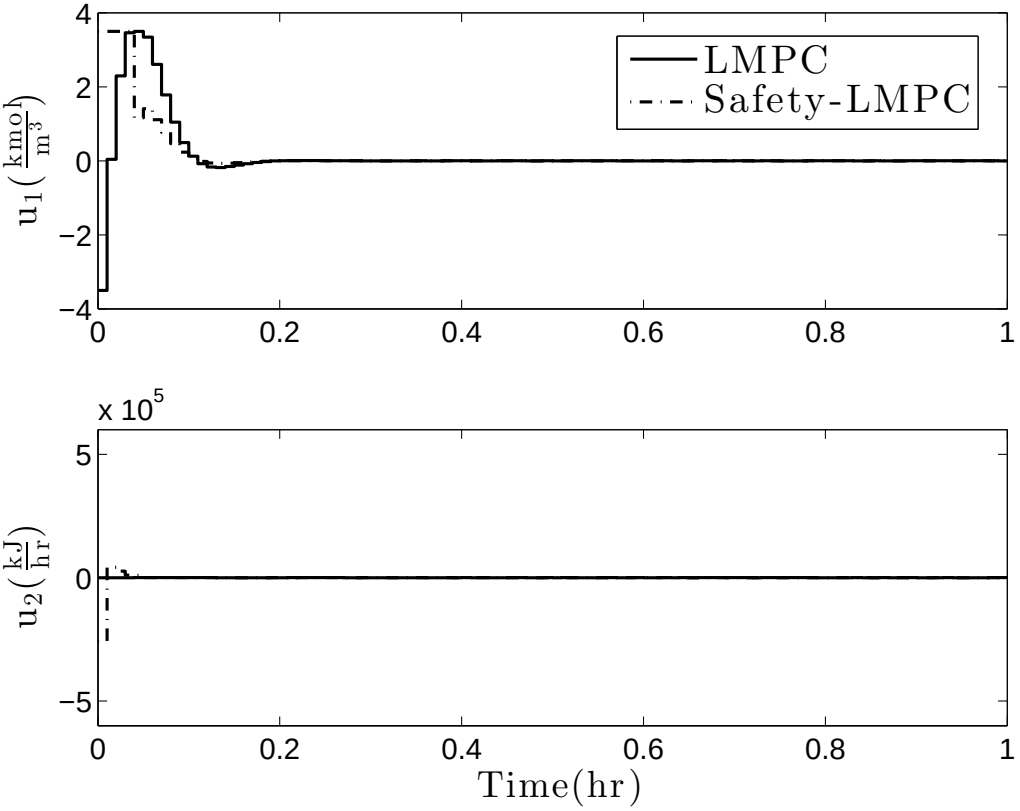

Figure 3.5: Manipulated input profiles for the closed-loop CSTR under the classical LMPC design of Eq. 3.6 and under the safety-LMPC design of Eq. 3.9 for the initial condition $x_{int} = [-1.42192\ \frac{kmol}{m^3}\ 22\ K]$ without process disturbances.

that drive the closed-loop state into the safety region quickly. Due to operation at the unstable steady-state, a Lyapunov-based controller of the form $h^T(x) = [h_1(x)\ h_2(x)]$ is constructed to estimate the stability region for the safety-LMPC 2. Also, a quadratic Lyapunov function $V(x) = x^T Px$ is used to construct the Lyapunov-based controller $h(x)$ where the weights of the P matrix were chosen to account for the different ranges of numerical values for each state. After extensive simulations, the P matrix was determined to be:

$$P = \begin{bmatrix} 850 & 18 \\ 18 & 3 \end{bmatrix}$$

To estimate the stability region Ω_ρ, the following feedback law (Sontag control law[59] is utilized

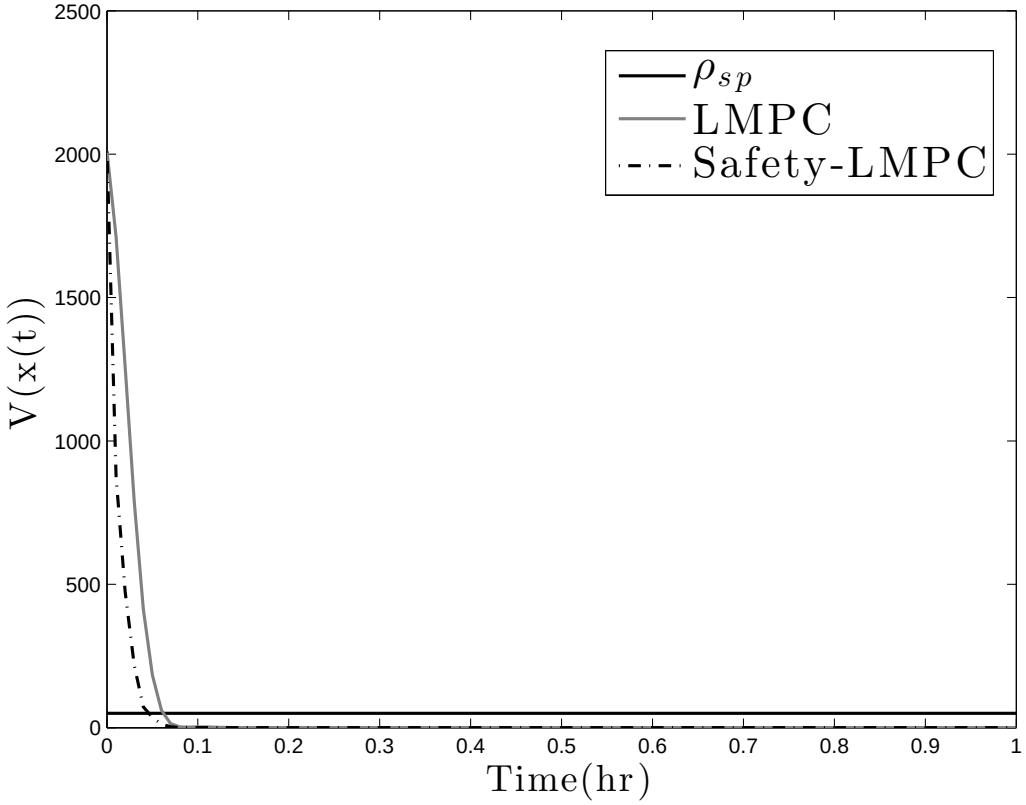

Figure 3.6: The Lyapunov function value with time for the closed-loop CSTR under the classical LMPC design of Eq. 3.6 and under the safety-LMPC design of Eq. 3.9 for the initial condition $x_{int} = [-1.42192 \ \frac{kmol}{m^3} \ 22 \ K]$ without process disturbances. The safety set-point ρ_{sp} is also shown.

for the inlet concentration and heat rate (i.e., $u_i = h_i(x), \ i = 1,2$):

$$h_i(x) = \begin{cases} -\dfrac{L_{\tilde{f}}V + \sqrt{L_{\tilde{f}}V^2 + L_{g_i}V^4}}{L_{g_i}V}, & \text{if } L_{g_i}V \neq 0 \\ 0, & \text{if } L_{g_i}V = 0 \end{cases} \tag{3.16}$$

where $L_{\tilde{f}}V$ and $L_{g_i}V$ are the Lie derivatives of the Lyapunov function $V(x)$ with respect to the vector fields $\tilde{f}(x)$ and $g_i(x)$ respectively. Both control laws are subject to input constraints. Under the control laws of Eq. 3.16 with input constraints, the stability region Ω_ρ is determined as a sufficiently large level set where the time-derivative of the Lyapunov function, $\dot{V}$, along the closed-loop state trajectories is negative. Figure 3.3 shows the methodology for choosing the stability

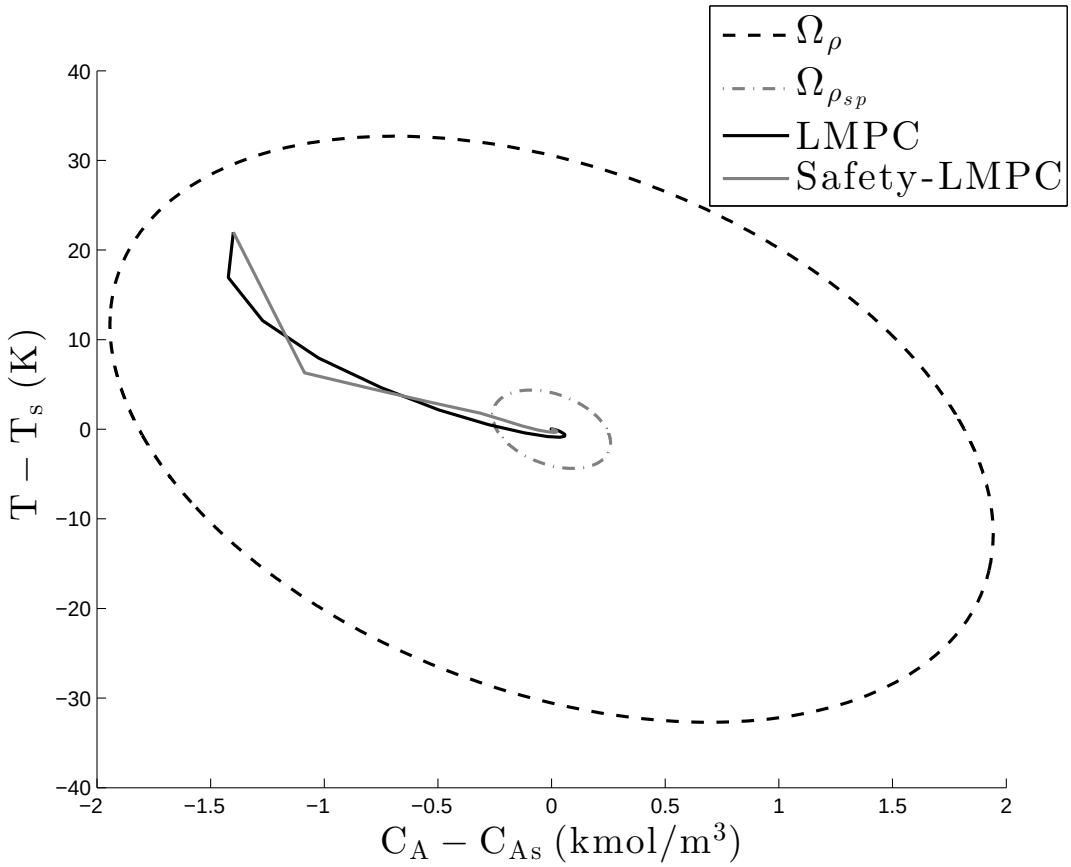

Figure 3.7: The state-space profile for the closed-loop CSTR under the classical LMPC design of Eq. 3.6 and under the safety-LMPC design of Eq. 3.9 for the initial condition $x_{int} = [-1.42192\ \frac{kmol}{m^3}\ 22\ K]$ without process disturbances.

region. Specifically, the state-space region shown in Figure 3.3 was discretized and the value of $\dot{V}$ along the closed-loop state trajectories of Eq. 3.14 under the control laws of Eq. 3.16 was evaluated at each discretized point. The grey region in Figure 3.3 is the open neighborhood around the origin where $\dot{V}$ is negative. After these extensive simulations, ρ was found with value 2800.

The process was initiated from an initial condition that is relatively far from the steady-state (i.e., $x(t_0) = x_{int} = [-1.42192\ \frac{kmol}{m^3}\ 22\ K]$, and $V(x(t_0)) = 2044.42$) at time t_0. At this time, it is determined that the process state must move quickly into a region where the temperature deviates from the steady-state value by no more than 4.33 K (i.e., $\rho_{sp} = 50$) to avoid an unsafe operating condition. For this scenario, the abilities of the safety-LMPC 2 and classical LMPC formulations are compared to meet this safety goal with and without process disturbances. Both controllers drive

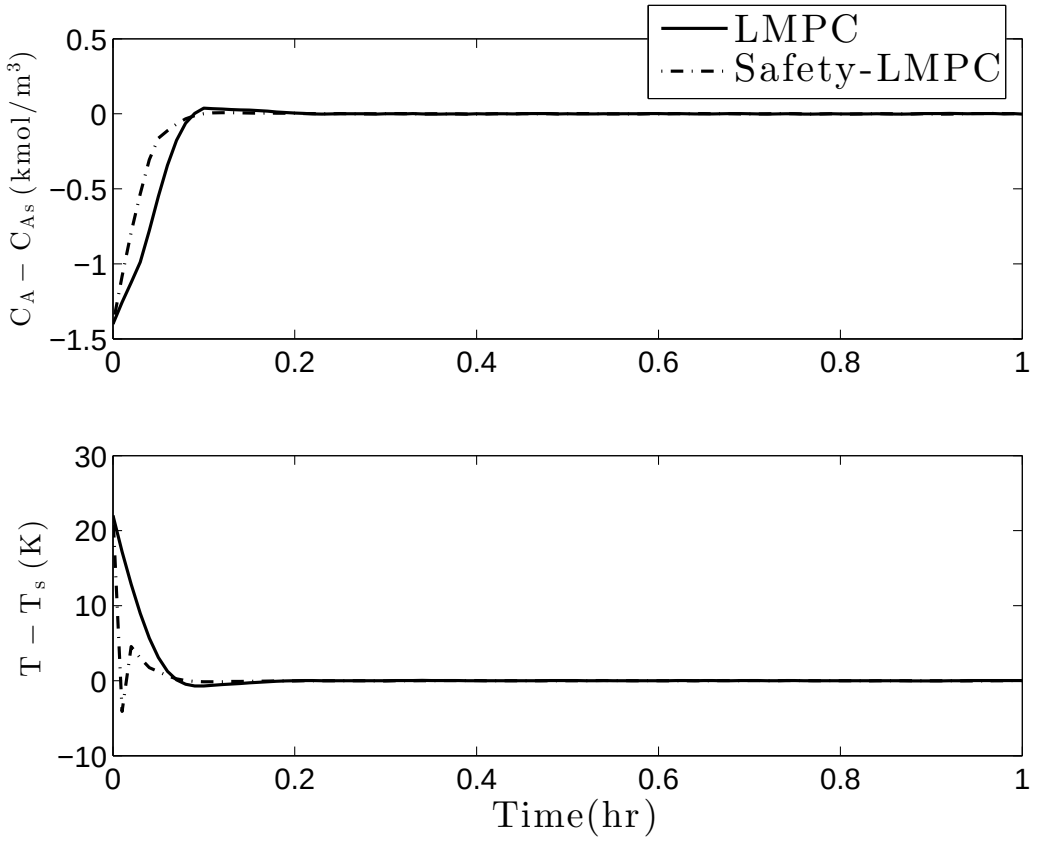

Figure 3.8: The state profiles for the closed-loop CSTR under the classical LMPC design of Eq. 3.6 and under the safety-LMPC design of Eq. 3.9 for the initial condition $x_{int} = [-1.42192\ \frac{kmol}{m^3}\ 22\ K]$ with process disturbances.

the closed-loop state toward the steady-state, but the safety-LMPC design accomplishes this while controlling the rate at which the closed-loop state converges to the steady-state. The safety-LMPC 2 and the classical LMPC formulations considered are both implemented with a prediction horizon $N = 10$, a sampling period $\Delta = 0.01\ hr$ and an operating period of length $t_f = 1\ hr$. The interior point solver Ipopt[90] was used to solve the optimization problems at each sampling time.

The safety-LMPC 2 formulation follows that in Eq. 3.9 with the objective function:

$$L(\tilde{x}, u, K_c) = \int_{t_k}^{t_{k+N}} [\tilde{x}(\tau)^T \tilde{x}(\tau) + u(\tau)^T u(\tau) + \frac{|\rho_{sp} - \tilde{\rho}(\tau)|^2}{h_c}] d\tau \tag{3.17}$$

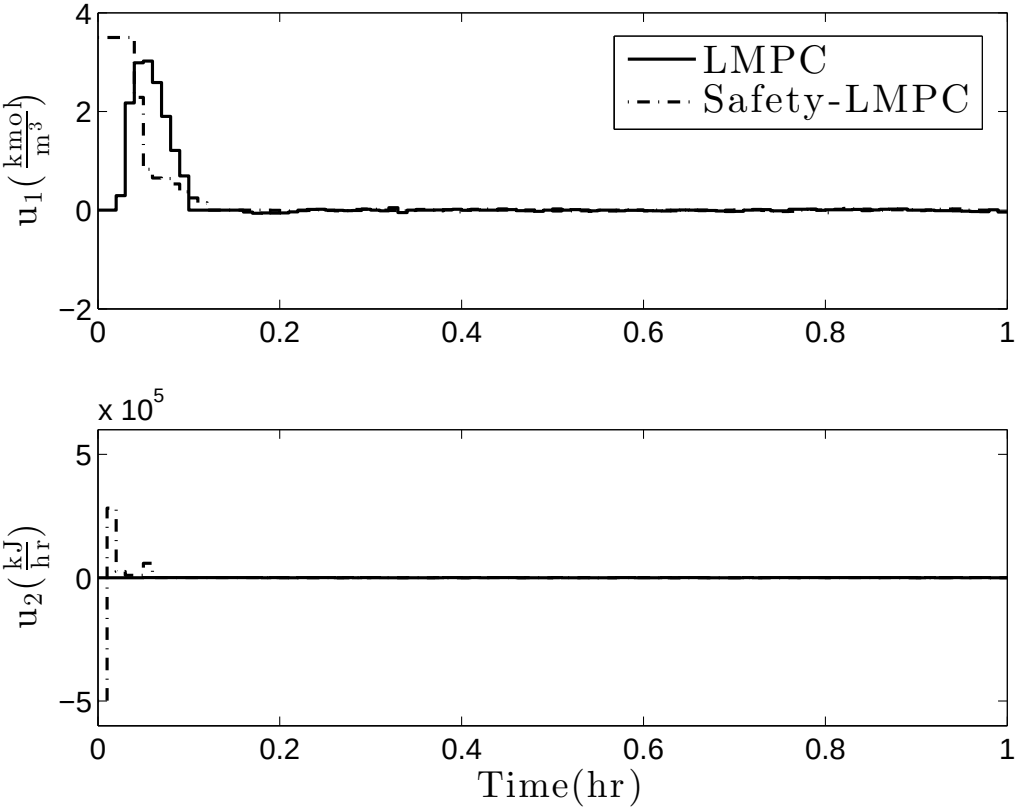

Figure 3.9: Manipulated input profiles for the closed-loop CSTR under the classical LMPC design of Eq. 3.6 and under the safety-LMPC design of Eq. 3.9 for the initial condition $x_{int} = [-1.42192\ \frac{kmol}{m^3}\ 22\ K]$ with process disturbances.

The first two terms of Eq. 3.17 are the objective function of the classical LMPC where the weighting matrices are

$$Q = R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

This weighting was chosen because it is considered that the heat input u_2 is costly, and since the magnitude of u_2 can be much larger than the magnitude of x or u_1, the specified weighting matrices prevent large values of u_2 from being requested and causing the value of Eq. 3.17 to become large. The third term in Eq. 3.17 is the safety penalty term where the the squared Euclidean norm is chosen to penalize the deviation of the Lyapunov function value of the predicted closed-loop state $\tilde{\rho}(t)$ from the safety set-point ρ_{sp}. The safety penalty term is significantly penalized by a large

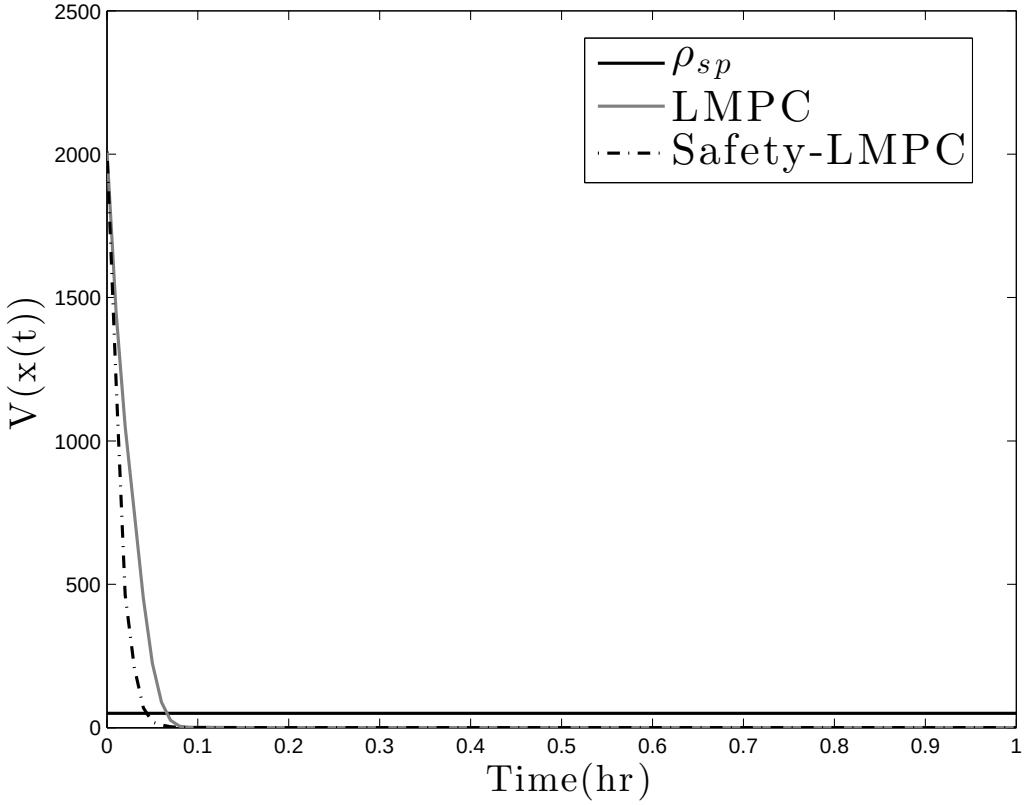

Figure 3.10: The Lyapunov function value with time for the closed-loop CSTR under the classical LMPC design of Eq. 3.6 and under the safety-LMPC design of Eq. 3.9 for the initial condition $x_{int} = [-1.42192 \ \frac{kmol}{m^3} \ 22 \ K]$ with process disturbances. The safety set-point ρ_{sp} is also shown.

weight $1/h_c$. Hence, the safety-LMPC 2 seeks to drive the closed-loop state into the safety region $\Omega_{\rho_{sp}}$ in a short time while using the minimum amount of energy u_2.

Figures 3.4-3.5 show the closed-loop state trajectories and the manipulated input trajectories of the CSTR, initiated from x_{int}, under the safety-LMPC scheme and the classical LMPC scheme without process disturbances. From Figure 3.4, the closed-loop state trajectory of the CSTR for the safety-LMPC 2 scheme reached the steady-state before that for the classical LMPC scheme. This is because the safety penalty term is highly penalized, which causes the closed-loop state to converge to the safety region more quickly than it does under the classical LMPC, and to then go to the steady-state. As shown in Figure 3.5, the safety-LMPC 2 utilized a large amount of energy (i.e., $u_2 = -2.6 \times 10^5 \ \frac{kJ}{hr}$) and the maximum amount of material (i.e., $u_1 = 3.5 \ \frac{kmol}{m^3}$) in the first sampling

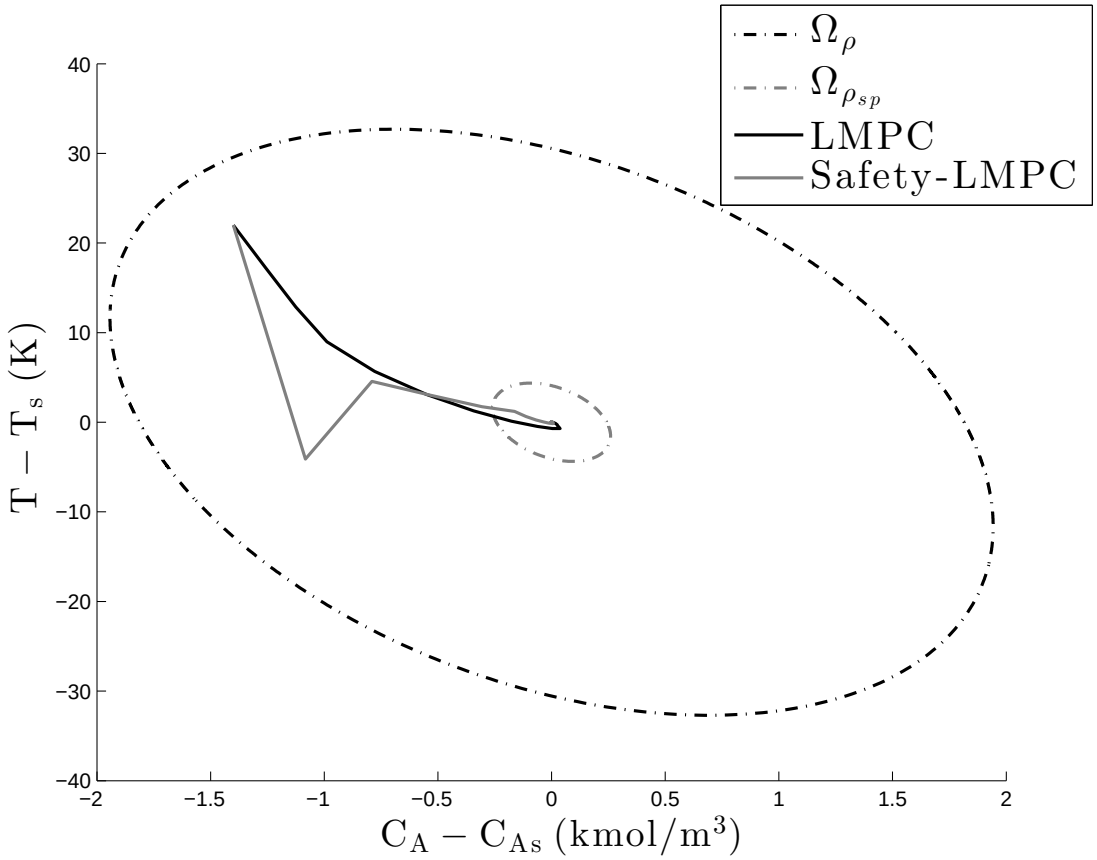

Figure 3.11: The state-space profile for the closed-loop CSTR under the classical LMPC design of Eq. 3.6 and under the safety-LMPC design of Eq. 3.9 for the initial condition $x_{int} = [-1.42192\ \frac{kmol}{m^3}\ 22\ K]$ with process disturbances.

period of the simulation to drive the closed-loop state into the safety region quickly due to the high weight on the safety penalty term. However, the classical LMPC used very little thermal energy (u_2) and less material (u_1) in the first sampling period of the simulation to minimize the value of the quadratic LMPC objective function.

Figures 3.6-3.7 depict the Lyapunov function value of the closed-loop state, and the state-space profile for the closed-loop state, under both the safety-LMPC 2 and the classical LMPC without process disturbances. In Figure 3.6, the closed-loop state under the safety-LMPC 2 entered the safety level set $\Omega_{\rho_{sp}}$ two sampling times before that under the classical LMPC. Figure 3.7 demonstrates that the state-space profile for the closed-loop state under the classical LMPC drove the closed-loop state to the safety region due to the combination of the contractive constraint and the

quadratic cost function of the classical LMPC. In addition, the safety-LMPC 2 scheme enhances the rate at which the closed-loop state approaches the safety region by the use of the safety penalty term and the safety-based constraints. After the closed-loop state trajectories under both schemes entered the safety region, they both reached the steady-state.

Figures 3.8-3.9 show the corresponding state and manipulated input profiles starting from the same initial condition but under bounded process disturbances ($w^T = [w_1 \; w_2]$ is the bounded disturbance vector corresponding to Gaussian white noise with variances $\sigma_1 = 1 \; \frac{kmol}{m^3}$ and $\sigma_2 = 40 \; K$) with $|w_1| \leq 1 \; \frac{kmol}{m^3}$ and $|w_2| \leq 40 \; K$. In the presence of disturbances, the safety-LMPC computes a value of u_1 that goes up to its allowable maximum value and u_2 reduces to its allowable minimum value in the first sampling period of the simulation to decrease the Lyapunov function value of the closed-loop state quickly, but the safety-LMPC eventually computes that both inputs should remain approximately at their steady-state values. Figures 3.10-3.11 show the Lyapunov function value of the closed-loop state, and the state-space profile for the closed-loop state, under both the safety-LMPC 2 and the classical LMPC under bounded process disturbances. In the presence of uncertainty, the closed-loop state under the safety-LMPC 2 entered the safety region two sampling times before that under the classical LMPC (Figure 3.10). Figure 3.11 and Figure 3.7 show that the closed-loop state trajectory under the safety-LMPC 2 chose a different path than the one for the classical LMPC, which led to an earlier entrance to the safety region by two sampling times in the presence and absence of uncertainty.

Remark 3.7 *The proposed control-safety system integration methodology (safety-LMPC) is demonstrated in the context of the traditional continuous stirred tank reactor (CSTR) example. The CSTR example uses a generic $A \rightarrow B$ reaction which corresponds to numerous industrial reactions. Generic reactions can be used to represent various industrial reactions including the production of propylene glycol from propylene oxide, which can be considered unsafe due to its exothermic nature and open-loop unstable steady-state (conceptually similar to the unstable steady-state analyzed for the CSTR of Eq. 3.14) from which open-loop deviations may result in the state moving toward a stable steady-state with a relatively high temperature. Therefore, incorporating safety-*

based constraints within the control system can reduce the number of alarms because the control system is now working to explicitly keep the closed-loop state in a safe region at all times.

3.5 Conclusion

In this chapter, two LMPC schemes with safety-based constraints were presented to integrate feedback control and process functional safety within a unified framework. The motivation for the proposed safety-LMPC design was given, in particular that it can be formulated to drive the closed-loop state to a safe region of operation at a desired rate, which cannot easily be accomplished by tuning the weighting matrices in the quadratic objective function. The safety-LMPC's vary the upper bound on the level set of the Lyapunov function to achieve the improved rate of approach to the safety region, and they can also be modified to shift the region of operation from a level set around one steady-state to a level set around another. For a sufficiently small sampling period, a proof of recursive feasibility and closed-loop stability of a class of nonlinear systems under one of the safety-LMPC formulations in the presence of uncertainty was given. The safety advantage of the safety-LMPC paradigm over the classical LMPC paradigm was illustrated through a chemical process example. Nevertheless, the safety-based controller design was developed with a centralized model predictive control (MPC) structure; thus, computation time limitations within a sampling period may reduce the effectiveness of such a controller design for promoting process safety. An alternative MPC architecture that is intended to improve the computation time of the MPC algorithm is a distributed model predictive control (DMPC) architecture.[28,84] This MPC architecture has been investigated for computation time benefits since it can reduce the number of decision variables in each of the distributed optimization problems and may be able to terminate the optimization problems before the optimal solution is found while maintaining feasibility and closed-loop stability of the controller. The next chapter presents a distributed Lyapunov-based model predictive control architecture formulated with safety-based constraints to decrease the computation time of the centralized safety-LMPC design.

Chapter 4

Distributed Economic Model Predictive Control for Operational Safety of Nonlinear Processes

4.1 Introduction

This chapter proposes the integration of a distributed model predictive control architecture with Lyapunov-based economic model predictive control (LEMPC) formulated with safety-based constraints. We consider both iterative and sequential distributed control architectures, and the partitioning of inputs between various optimization problems in the distributed structure based on their impact on process operational safety. Moreover, sufficient conditions that ensure feasibility and closed-loop stability of the iterative and sequential safety distributed LEMPC designs are given. A comparison between the proposed safety distributed EMPC controllers and the safety centralized EMPC is demonstrated via a chemical process example. The results of this chapter originally appeared in.[9]

4.2 Preliminaries

4.2.1 Notation

The operator $|\cdot|$ denotes the Euclidean norm of a vector. x^T represents the transpose of a vector x. The symbol Ω_ρ is used to represent a level set of a sufficiently smooth, positive definite scalar-valued function $V(x)$ and is defined by $\Omega_\rho := \{x \in R^n : V(x) \leq \rho\}$. The operator '/' denotes set subtraction, that is, $A/B := \{x \in R^n : x \in A, x \notin B\}$. The symbol $S(\Delta)$ denotes the family of piecewise constant, right-continuous functions with a fixed time interval $\Delta \geq 0$. A diagonal matrix which has the components of a vector v as its diagonal elements is denoted by the symbol $\text{diag}(v)$. A function $\alpha : [0,a) \to [0,\infty)$ with $\alpha(0) = 0$ belongs to class $\mathscr{K}$ if it is continuous and strictly increasing.

4.2.2 Class of Nonlinear Process Systems

In this chapter, we consider a nonlinear process system with the following state-space description:

$$\dot{x} = f(x) + \sum_{i=1}^{m} g_i(x)\bar{u_i} + b(x)w \tag{4.1}$$

where $x \in \mathbb{R}^n$ and $w \in \mathbb{R}^{n_w}$ are the state and disturbance vectors, respectively. Due to the implementation strategy of the proposed safety-based DEMPC, the full input vector is divided into m input vectors where the i^{th} manipulated input vector is denoted by $\bar{u_i} \in \mathbb{R}^{m_i}$ for $i = 1,\ldots,m$, and each of these input vectors is bounded in a convex set U_i (i.e., $U_i := \{\bar{u_i} \in \mathbb{R}^{m_i} : |\bar{u_i}| \leq \bar{u_i}^{max}\},\ i = 1,\ldots,m$, where the $\bar{u_i}^{max}$, $i = 1,\ldots,m$, represent the magnitudes of the input constraints). The vector functions f, g_i, $i = 1,\ldots,m$, and b are assumed to be locally Lipschitz vector functions of their arguments. Furthermore, it is assumed that the state of the system of Eq. 4.1 is synchronously sampled at time instances $t_k = t_0 + k\Delta,\ k = 0,1,\ldots$, where t_0 is the initial time. The vector w is bounded within the set $W := \{w \in \mathbb{R}^{n_w} |\ |w| \leq \theta,\ \theta > 0\}$ (i.e., $w \in W$). We assume that the origin is an equilibrium point of the unforced nominal system (i.e., $f(0) = 0,\ g_i(0) = 0,\ i = 1,\ldots,m$, and

$b(0) = 0$).

Remark 4.1 *The systems of equations describing the behavior of many chemical process systems are of the form of Eq. 4.1. For those that are not, the distributed safety-based controller formulations developed in this chapter can still be utilized, but the closed-loop stability and feasibility results presented may not hold.*

4.2.3 Stabilizability Assumption

We consider systems of the form of Eq. 4.1 for which Assumption 4.1 (stabilizability assumption) holds.

Assumption 4.1 *There exists a locally Lipschitz feedback control law* $\bar{h}^T(x) = [\bar{h}_1(x) \ \ldots \ \bar{h}_m(x)]$ *with* $\bar{h}(0) = 0$ *for the nominal closed-loop system of Eq. 4.1 (i.e.,* $w(t) \equiv 0$*) that renders the origin of the nominal system of Eq. 4.1 under* $\bar{u}_i = \bar{h}_i(x)$, $i = 1, \ldots, m$, *asymptotically stable for all* $x \in D \subseteq R^n$, *where D is an open neighborhood of the origin, when applied continuously in the sense that there exists a continuously differentiable Lyapunov function* $V(x)$[49,63] *for the nominal closed-loop system and class* $\mathcal{K}$ *functions* $\alpha_i(\cdot)$, $i = 1,2,3,4$, *such that the following inequalities hold:*

$$\alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|) \tag{4.2a}$$

$$\frac{\partial V(x)}{\partial x}(f(x) + \sum_{i=1}^{m} g_i(x)\bar{h}_i(x)) \leq -\alpha_3(|x|) \tag{4.2b}$$

$$\left|\frac{\partial V(x)}{\partial x}\right| \leq \alpha_4(|x|) \tag{4.2c}$$

$$\bar{h}_i(x) \in U_i, i = 1, \ldots, m \tag{4.2d}$$

The stability region of the closed-loop system under the feedback control law that meets Assumption 4.1 is defined as a level set of the Lyapunov function within D where Eq. 4.2 holds, and it is denoted by Ω_ρ.

By continuity, the local Lipschitz property assumed for the vector fields f, g_i, $i = 1,\ldots,m$, and b, the continuous differentiability property of the Lyapunov function $V(x)$, and taking into account that the manipulated inputs $u_i,\ i = 1,\ldots,m$, and the disturbances w are bounded in convex sets, there exist positive constants $L_w,\ L_x,\ L_{\bar{u_i}},\ i = 1,\ldots,m$, and M such that

$$\left| f(x) + \sum_{i=1}^{m} g_i(x)\bar{u_i} + b(x)w \right| \leq M \tag{4.3}$$

$$\left| \frac{\partial V}{\partial x} f(x) - \frac{\partial V}{\partial x} f(x') \right| \leq L_x \left| x - x' \right| \tag{4.4}$$

$$\left| \frac{\partial V}{\partial x} g_i(x) - \frac{\partial V}{\partial x} g_i(x') \right| \leq L_{\bar{u_i}} \left| x - x' \right|,\ i = 1,\ldots,m \tag{4.5}$$

$$\left| \frac{\partial V}{\partial x} b(x) \right| \leq L_w \tag{4.6}$$

for all $x, x' \in \Omega_\rho$, $\bar{u_i} \in U_i$, $i = 1,\ldots,m$, and $w \in W$.

4.2.4 Centralized Safety-Based LEMPC

In the centralized Safety-LEMPC design of Eq. 4.7b presented in Chapter 2, the control actions for all m input vectors are computed together in one optimization problem.[6] The centralized Safety-

LEMPC controller design for the nonlinear system of Eq. 4.1 is formulated as follows:

$$\max_{\bar{u}_1,\ldots,\bar{u}_m,K_c\in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau),\bar{u}_1(\tau),\ldots,\bar{u}_m(\tau)) - \tag{4.7a}$$

$$\phi(\rho_{sp}-\tilde{\rho}(\tau))d\tau$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t)) + \sum_{i=1}^{m} g_i(\tilde{x}(t))\bar{u}_i \tag{4.7b}$$

$$\bar{u}_i(t) \in U_i,\ i=1,\ldots,m,\ \forall\, t\in[t_k,t_{k+N}) \tag{4.7c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{4.7d}$$

$$K_c(t) \geq 0,\ \forall\, t\in[t_k,t_{k+N}) \tag{4.7e}$$

$$V(\tilde{x}(t)) \leq \tilde{\rho}(t),\ \forall\, t\in[t_k,t_{k+N}) \tag{4.7f}$$

$$\frac{d\tilde{\rho}}{dt} = K_c(t)(\rho_{sp}-\tilde{\rho}(t)) \tag{4.7g}$$

$$\tilde{\rho}(t_k) = V(x(t_k)), \quad \text{if } x(t_k)\notin\Omega_{\rho_{sp}}$$

$$\tilde{\rho}(t_k) = \rho_{sp}, \quad \text{if } x(t_k)\in\Omega_{\rho_{sp}}$$

$$\frac{\partial V(x(t_k))}{\partial x}\Big(\sum_{i=1}^{m} g_i(x(t_k))\bar{u}_i(t_k)\Big) \tag{4.7h}$$

$$\leq \frac{\partial V(x(t_k))}{\partial x}\Big(\sum_{i=1}^{m} g_i(x(t_k))\bar{h}_i(x(t_k))\Big),$$

$$\text{if } x(t_k)\in\Omega_\rho/\Omega_{\bar{\rho}_{sp}} \text{ or } t_k > t_s$$

where the optimization variables are the piecewise-constant input trajectories $\bar{u}_i(t),\ldots,\bar{u}_m(t)$, over the prediction horizon $N\Delta$, as well as the piecewise-constant auxiliary variable $K_c(t)$ that plays a role in the safety-based constraints. L_e is a cost function that is determined based on economic considerations and is not required to have its minimum at a steady-state. The Safety-LEMPC formulation is a variation on the LEMPC formulation developed in[43] that has been augmented with safety-based constraints, and as a result it contains many of the standard constraints utilized in EMPC (e.g., a nominal process model for the predicted state $\tilde{x}$ (Eq. 4.7b), input constraints (Eq. 4.7c), and state feedback (Eq. 4.7d)). The time t_s represents a time after which the constraint

of Eq. 4.7h is active for all subsequent times.

The motivation for adding safety-based constraints to this formulation is that situations may arise in which parts of Ω_ρ become unsafe to operate within due to, for example, prolonged closed-loop operation in a high-temperature region of state-space or expected effects from process disturbances. In such cases, a safety logic unit that determines the safest level set of V for the process to operate within may find that the closed-loop state should enter and remain within the set $\Omega_{\rho_{sp}}$, $\rho_{sp} < \rho$, to avoid unsafe scenarios. The safety level set $\Omega_{\rho_{sp}}$ is determined based on data on the probability of potential failures of process equipment, control system failures and measurement sampling time of the process state.[6] To drive the closed-loop state rapidly into $\Omega_{\rho_{sp}}$ while maintaining feasibility of the optimization problem, safety-based constraints (Eqs. 4.7e-4.7h) are added to the LEMPC, in addition to adding a penalty term $\phi(\rho_{sp} - \tilde{\rho}(\tau))$ to the objective function of Eq. 4.7a, that penalizes the difference between the the upper bound of the Lyapunov function $\tilde{\rho}(\tau)$ and ρ_{sp}. The function $\phi(\cdot)$ is selected based on the need to drive the process state into the safety region; for example, $\phi(\cdot) = |\cdot|^2$ is a potential function since its minimum occurs with $\rho_{sp} = \tilde{\rho}_{sp}$. When the penalty term is significant, the Safety-LEMPC will seek to find trajectories for $\bar{u_i}(t)$, $i = 1, \ldots, m$, and $K_c(t)$ that drive the predicted closed-loop state into $\Omega_{\rho_{sp}}$ more quickly than without the penalty and dynamic constraints of Eqs. 4.7e-4.7h. Specifically, to decrease $\tilde{\rho}(t)$ from Eq. 4.7g toward ρ_{sp} to minimize the objective function including ϕ, a positive value of $K_c(t)$ (Eq. 4.7e) is computed for which inputs $\bar{u_i}(t)$, $i = 1, \ldots, m$, are found to decrease $V(\tilde{x}(t))$ at a rate that allows Eq. 4.7f to be satisfied at all times given the rate of decrease of $\tilde{\rho}$ from Eq. 4.7g. The constraint of Eq. 4.7h (contractive constraint) forces the time derivative of the Lyapunov function under the Safety-LEMPC to be less than or equal to the time derivative of the Lyapunov function under the explicit stabilizing controller $\bar{h}(x)$. A subset of the safety level set $\Omega_{\bar{\rho}_{sp}}$ activates the contractive constraint of Eq. 4.7h and should be chosen to make $\Omega_{\rho_{sp}}$ an invariant set.[6]

4.3 Safety-Distributed-LEMPC

For large-scale industrial nonlinear process systems, the time required to solve the centralized Safety-LEMPC design of Eq. 4.7 with the full process model and potentially tens or hundreds of optimization variables may be large. Therefore, a large sampling period in the LEMPC may be required. However, the closed-loop stability, feasibility, and safety-related proofs in[6] hold only for a sufficiently small sampling period and sufficiently small disturbances. Furthermore, even if the sampling period is sufficiently small to ensure that closed-loop stability within Ω_ρ is guaranteed, the length of the sampling period affects the minimum size of the level set of the stability region into which the closed-loop state is driven under repeated application of the contractive constraint.[43] This minimum size level set corresponds to the minimum size of a safe level set of operation that can be chosen within the stability region. To improve process safety, it is desirable to be able to make the safety region as small as possible (i.e., to be able to decrease the sampling period to a small value) to provide great flexibility in handling unsafe scenarios. When the time required to solve the centralized Safety-LEMPC is high, the computation time issue cannot be handled with decentralized control designs (i.e., multiple controllers utilize the same process model to compute subsets of the entire set of available control actions without communication between the controllers), because such designs may pose safety concerns since the controllers do not coordinate their actions.[56] However, a distributed Safety-LEMPC design (i.e., multiple controllers utilize the same process model to compute subsets of the entire set of available control actions but the controllers communicate) can be used to address the computation time concerns. Therefore, both sequential and iterative distributed Safety-LEMPC designs are proposed in this chapter.

Remark 4.2 *In this chapter, we assume that the upper bound on the disturbance is known, and thus we appeal to the conditions guaranteeing closed-loop stability and feasibility from[6] to motivate the use of distributed Safety-LEMPC. However, in industry, it is more common that the upper bound on the disturbance is estimated but not known, and in that case reducing the computation time of Safety-LEMPC using a distributed architecture has the safety benefit of allowing more frequent*

feedback to reduce the likelihood that the closed-loop state will exit the safety level set during a sampling period if a large disturbance potentially greater than the expected/typical bound affects the process. However, further discussion of this point is outside the scope of this chapter.

4.3.1 Safety-Sequential-DLEMPC

A sequential design for a distributed Safety-LEMPC (Safety-S-DLEMPC) involves a hierarchy of m controllers, each of which solves the optimization problem in Eq. 4.7 but optimizes only $\bar{u}_i$ for a given $i \in \{1,\dots,m\}$ and assumes a value of the other inputs. The designation "sequential" arises because the controllers are connected in series. The i^{th} controller in the hierarchy (which we will refer to as Safety-S-DLEMPC i) assumes the values of $\bar{u}_p$, $p = 1,\dots,i-1$, throughout the prediction horizon calculated by the controllers higher up in the hierarchy, and the values $\bar{u}_p(t) = \bar{h}_p(x(t_q))$, $p = i+1,\dots,m$, $\forall\ t \in [t_q, t_{q+1})$, $q = k,\dots,k+N-1$, for the rest of the control inputs when calculating $\bar{u}_i$. The optimal input trajectory for $\bar{u}_i$ determined for Safety-S-DLEMPC i at t_k is denoted by $\bar{u}_i^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $i = 1,\dots,m$. Two considerations with respect to the distributed control design are: (1) whether it is necessary to solve for K_c in all m Safety-S-DLEMPC's, and (2) how to decide which inputs should be placed within $\bar{u}_1$, which within $\bar{u}_2$, and so on. To address these points, the main results of the proof of feasibility and closed-loop stability for the Safety-S-DLEMPC will be utilized.

To determine the number of distributed controllers that must solve for K_c, consider first the case that all m distributed controllers solve for K_c. First, Safety-S-DLEMPC 1 solves Eq. 4.7 for the piecewise-constant trajectories for $\bar{u}_1$ and K_c throughout the prediction horizon and sets $[\bar{u}_2(t),\dots,\bar{u}_m(t)]$ to the corresponding $[\bar{h}_2(x(t_q)),\dots,\bar{h}_m(x(t_q))]$, $\forall\ t \in [t_q, t_{q+1})$, $q = k,\dots,k+N-1$. The input trajectory $\bar{u}_1(t) = \bar{h}_1(x(t_q))$, $\forall\ t \in [t_q, t_{q+1})$, $q = k,\dots,k+N-1$, and the gain $K_c = 0$, $\forall\ t \in [t_k, t_{k+N})$, is a feasible solution to the resulting optimization problem because it satisfies all constraints. Therefore, there is always a feasible solution to Safety-S-DLEMPC 1. Now, consider that Safety-S-DLEMPC 2 receives the optimal trajectory of $\bar{u}_1$ throughout the prediction horizon from Safety-S-DLEMPC 1, sets $[\bar{u}_3(t),\dots,\bar{u}_m(t)] = [\bar{h}_3(x(t_q)),\dots,\bar{h}_m(x(t_q))]$, $\forall\ t \in [t_q, t_{q+1})$,

$q = k, \ldots, k+N-1$, and solves for both the trajectory of $\bar{u}_2$ and of K_c. When $\bar{u}_2(t) = \bar{h}_2(x(t_q))$, $\forall\, t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$, all inputs $\bar{u}_i$, $i = 1, \ldots, m$, take the same values as they did for the optimal solution of Safety-S-DLEMPC 1 and the problem is feasible, assuming that K_c also takes the same trajectory as for that optimal solution. Therefore, a feasible solution to safety-S-DLEMPC 2 exists, which is the same as the feasible solution to Safety-S-DLEMPC 1. Recursively applying such arguments to Safety-S-DLEMPC 3 through Safety-S-DLEMPC m shows that each optimization problem in the Safety-S-DLEMPC structure has a feasible solution, and that the final solution satisfies Eqs. 4.7f and 4.7h with $\bar{u}_1^*(t|t_k), \ldots, \bar{u}_m^*(t|t_k)$, $\forall\, t \in [t_k, t_{k+N})$. When Eq. 4.7h is satisfied throughout a sampling period, then given a sufficiently small Δ and a sufficiently small θ, and due to Eq. 4.2b, the distributed Safety-S-DLEMPC architecture will cause the Lyapunov function value to decrease between two sampling periods when $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$ until it reaches the safety region.[43] Due to the safety penalty term in the objective function and safety-based constraints, there is a possibility that the rate at which $V(x)$ decreases along the closed-loop state trajectories under the Safety-S-DLEMPC paradigm may be faster than under a distributed LEMPC paradigm without safety-based constraints; however, in general, no guarantee can be made regarding this, and no proof can even be made regarding whether the rate of approach is the fastest rate that was obtained in any one of the m Safety-S-DLEMPC optimization problems.

The above discussion shows that if K_c is solved in all m Safety-S-DLEMPC's of the distributed architecture, then the Safety-S-DLEMPC is guaranteed to cause the closed-loop state to enter the safety region in finite time and to remain there. In the above discussion, it was noted that $K_c = 0$ allowed a feasible solution in each Safety-S-DLEMPC, but potentially a less restrictive solution than if the value of K_c was allowed to be positive. Therefore, it is possible to set $K_c = 0$ (i.e., remove K_c as an optimization variable) for some subset of the m Safety-S-DLEMPC's to reduce the number of optimization variables in some of these controllers when that provides a computation time benefit. The resulting control actions may not decrease the Lyapunov function as quickly as if K_c was optimized; however, if the inputs in the vector $\bar{u}_i$, for some $i \in \{1, \ldots, m\}$, have very little impact on the value of $V(\tilde{x})$ throughout the prediction horizon, the result of solving Safety-S-

DLEMPC both including K_c as an optimization variable and the result with $K_c \equiv 0$ may produce similar results because the vector $\bar{u}_i$ is not able to affect the safety penalty term in the objective function highly. This implies that grouping inputs with regard to their impact on process safety may be beneficial for helping to reduce the number of optimization variables in some of the m Safety-S-DLEMPC problems. However, the full effects of the input partitioning and of setting $K_c = 0$ in some optimization problems should be evaluated through closed-loop simulations.

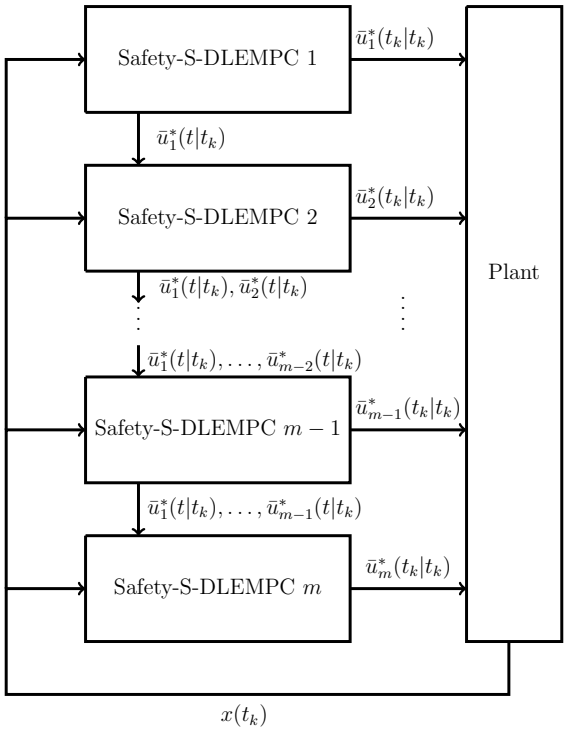

Figure 4.1: Block diagram of the Safety-S-DLEMPC scheme

A schematic of the sequential distributed safety-based LEMPC architecture with m controllers is shown in Figure 4.1. Safety-S-DLEMPC j calculates an input vector $\bar{u}_j$ where $\bar{u}_j^*(\tau|t_k),\ \tau \in [t_k, t_{k+N})$ denotes the optimal solution of Safety-S-DLEMPC j at time t_k. Safety-S-DLEMPC j may calculate the gain K_c as well throughout the prediction horizon (the trajectory of the optimal gain throughout the prediction horizon calculated by Safety-S-DLEMPC j at time t_k is denoted by $K_c^*(\tau|t_k),\ \tau \in [t_k, t_{k+N})$; it is not shown in Figure 4.1 because it is not communicated to the other Safety-S-DLEMPC controllers). The implementation strategy for the Safety-S-DLEMPC design is summarized as follows:

1. At t_k, all Safety-S-DLEMPC controllers receive a measurement of the current state $x(t_k)$ from the sensors. Go to Step 2.

2. For $j = 1$ to m:

   (a) Safety-S-DLEMPC j receives the set of input trajectories $\overline{u}_p^*(\tau|t_k),\ \tau \in [t_k, t_{k+N}),\ p = 1,\ldots,j-1$, from Safety-S-DLEMPC $j-1$ and assumes the input trajectories $\overline{u}_r(t) = \overline{h}_r(x(t_q)),\ t \in [t_q, t_{q+1}),\ q = k,\ldots,k+N-1$, for $r = j+1,\ldots,m$. Based on these input trajectories and $x(t_k)$, Safety-S-DLEMPC j evaluates the input trajectory of $\overline{u}_j$ and, when $K_c \not\equiv 0$, the trajectory of the gain K_c. If $j \neq m$, go to Step 2b. Else, go to Step 2c.

   (b) Safety-S-DLEMPC j sends $\overline{u}_p^*(\tau|t_k)$, $\tau \in [t_k, t_{k+N})$, $p = 1,\ldots,j$, to Safety-S-DLEMPC $j+1$. Go to Step 2a.

   (c) Go to Step 3.

3. Each Safety-S-DLEMPC sends its optimal solution for the first sampling period of the prediction horizon to its actuator (i.e., all $u_i^*(t_k|t_k)$, $i = 1,\ldots,m$, are implemented on the process). Go to Step 4.

4. When a new state measurement is received at t_{k+1}, go to Step 1 ($k \leftarrow k+1$).

The formulation of Safety-S-DLEMPC j is as follows:

$$\max_{\bar{u}_j, K_c \in S(\Delta)} \int_{t_k}^{t_{k+N}} [L_e(\tilde{x}^j(\tau), \bar{u}_1(\tau), \ldots, \bar{u}_m(\tau)) - \tag{4.8a}$$

$$\phi(\rho_{sp} - \tilde{\rho}(\tau))] d\tau$$

$$\text{s.t. } \dot{\tilde{x}}^j(t) = f(\tilde{x}^j(t)) + \sum_{i=1}^{m} g_i(\tilde{x}^j(t)) \bar{u}_i(t) \tag{4.8b}$$

$$\bar{u}_j(t) \in U_j, \ \forall\, t \in [t_k, t_{k+N}) \tag{4.8c}$$

$$\bar{u}_r(t) = \bar{h}_r(\tilde{x}^j(t_{k+q})), \ r = j+1, \ldots, m, \ \forall\, t \in [t_{k+q}, t_{k+q+1}),$$

$$q = 0, \ldots, N-1 \tag{4.8d}$$

$$\bar{u}_p(t) = \bar{u}_p^*(t|t_k), \ p = 1, \ldots, j-1, \ \forall\, t \in [t_k, t_{k+N}) \tag{4.8e}$$

$$\tilde{x}^j(t_k) = x(t_k) \tag{4.8f}$$

$$K_c(t) \geq 0, \ \forall\, t \in [t_k, t_{k+N}) \tag{4.8g}$$

$$V(\tilde{x}^j(t)) \leq \tilde{\rho}(t), \ \forall\, t \in [t_k, t_{k+N}) \tag{4.8h}$$

$$\frac{d\tilde{\rho}}{dt} = K_c(t)(\rho_{sp} - \tilde{\rho}(t)) \tag{4.8i}$$

$$\tilde{\rho}(t_k) = V(x(t_k)), \quad \text{if } x(t_k) \notin \Omega_{\rho_{sp}}$$

$$\tilde{\rho}(t_k) = \rho_{sp}, \quad \text{if } x(t_k) \in \Omega_{\rho_{sp}}$$

$$\frac{\partial V(x(t_k))}{\partial x} \Big(\sum_{i=1}^{m} g_i(x(t_k)) \bar{u}_i(t_k) \Big) \tag{4.8j}$$

$$\leq \frac{\partial V(x(t_k))}{\partial x} \Big(\sum_{i=1}^{m} g_i(x(t_k)) \bar{h}_i(x(t_k)) \Big),$$

$$\text{if } x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}} \text{ or } t_k > t_s$$

where $\tilde{x}^j(t)$ denotes the predicted state trajectory under Safety-S-DLEMPC j. The values of the inputs $\bar{u}_r, \ r = j+1, \ldots, m$, that have not yet been computed by a Safety-S-DLEMPC are set to the corresponding elements of $\bar{h}(x)$ applied in a sample-and-hold fashion by the constraint of Eq. 4.8d. The trajectories of $\bar{u}_p$, $p = 1, \ldots, j-1$, are set to the optimal trajectories $\bar{u}_p^*(t|t_k)$, $t \in [t_k, t_{k+N})$, calculated by the Safety-S-DLEMPC's $p = 1, \ldots, j-1$, by the constraint of Eq. 4.8e. The other

constraints of the optimization problem of Eq. 4.8 follow those in Eq. 4.7.

If K_c is set to zero in Safety-S-DLEMPC j, the controller will only solve for the input vector $\bar{u}_j$. As a result, the objective function of Eq. 4.8a will only include the economic cost $L_e(\tilde{x}^j(\tau), \bar{u}_1(\tau), \ldots, \bar{u}_m(\tau))$. When $K_c(t) \equiv 0$, $\forall\ t \in [t_k, t_{k+N})$, the constraints of Eqs. 4.8h-4.8i reduce to:

$$V(\tilde{x}^j(t)) \leq \tilde{\rho},\ \forall\, t \in [t_k, t_{k+N})$$

$$\tilde{\rho} = V(x(t_k)), \quad \text{if } x(t_k) \notin \Omega_{\rho_{sp}}$$

$$\tilde{\rho} = \rho_{sp}, \quad \text{if } x(t_k) \in \Omega_{\rho_{sp}}$$

The contractive constraint of Eq. 4.8j will also be imposed in the Safety-S-DLEMPC that only solves for the input vector $\bar{u}_j$. This constraint guarantees that regardless of the value of K_c, the closed-loop state can be driven to the safety level set $\Omega_{\rho_{sp}}$ and maintained within that set thereafter (as will be shown below in the proof of Theorem 4.1).

We will now prove recursive feasibility and closed-loop stability of the Safety-S-DLEMPC implementation strategy, with the design of Safety-S-DLEMPC j following Eq. 4.8, and allowing for $K_c \equiv 0$ in any of the m Safety-S-DLEMPC's as desired. To proceed with this analysis, we first state a proposition that describes the closed-loop stability properties of the Lyapunov-based controller utilized in defining constraints of the Safety-S-DLEMPC design of Eq. 4.8.

Proposition 4.1 (c.f.[72]) *Consider the trajectory $\hat{x}(t)$ of the system of Eq. 4.1 in closed-loop for a controller $\bar{h}(x)$, which satisfies the condition of Eq. 4.2, obtained by solving recursively:*

$$\dot{\hat{x}}(t) = f(\hat{x}(t)) + \sum_{i=1}^{m} g_i(\hat{x}(t))\bar{h}_i(\hat{x}(t_k)) + b(x(t))w(t) \tag{4.9}$$

where $t \in [t_k, t_{k+1})$ with $k = 0, 1, \ldots$. Let $\Delta, \varepsilon_w > 0$ and $\rho > \rho_s > 0$ satisfy:

$$-\alpha_3(\alpha_2^{-1}(\rho_s)) + (L_x + \sum_{i=1}^{m} L_{\bar{u}_i}\bar{u}_i^{max})M\Delta + L_w\theta \leq -\varepsilon_w/\Delta. \tag{4.10}$$

Then, if $\hat{x}(t_0) \in \Omega_\rho$ *and* $\rho_{\min} < \rho$ *where*

$$\rho_{\min} = \max\{V(x(t+\Delta)) : V(x(t)) \leq \rho_s\}, \tag{4.11}$$

the following inequality holds:

$$V(\hat{x}(t_k)) \leq \max\{V(\hat{x}(t_0)) - k\varepsilon_w, \rho_{\min}\}. \tag{4.12}$$

Proposition 4.1 guarantees several points regarding operation of the closed-loop system under $\bar{h}(x)$ implemented in sample-and-hold, namely that with a sufficiently small sampling period and bound on the disturbance such that Eq. 4.10 is satisfied: 1) If $\hat{x}(t_k) \in \Omega_\rho$, then $\hat{x}(t_{k+1}) \in \Omega_\rho$, 2) if $\hat{x}(t_k) \in \Omega_\rho / \Omega_{\rho_s}$, then $V(\hat{x}(t_{k+1})) < V(\hat{x}(t_k))$, and 3) if $\hat{x}(t_k)$ enters Ω_{ρ_s}, $\hat{x}(t)$ obtained from recursively solving Eq. 4.9 remains within $\Omega_{\rho_{\min}}$ (ultimate boundedness of the closed-loop state of Eq. 4.9 within $\Omega_{\rho_{\min}}$). We note that $\rho_{\min}$ is defined in Eq. 4.11 with respect to the state $x(t)$ in Eq. 4.1, rather than with respect to the state under $\bar{h}(x)$ as in Eq. 4.9 (i.e., $\rho_{\min}$ is defined with respect to the worst-case deviation of $V(x)$ from ρ_s throughout a sampling period given Δ, θ, and $\bar{u}_i^{max}$, $i = 1, \ldots, m$, and does not assume any specific feedback control law in its definition)..

The following theorem provides sufficient conditions under which the Safety-S-DLEMPC design of Eq. 4.8 guarantees recursive feasibility and closed-loop stability of the system of Eq. 4.1.

Theorem 4.1 *Consider the system of Eq. 4.1 in closed-loop under the sequential distributed safety-based LEMPC design of Eq. 4.8 based on a controller* $\bar{h}(x)$ *that satisfies the conditions of Eq. 4.2. Let* $\varepsilon_w > 0$, $\Delta > 0$, $\rho > \rho_{sp} > \bar{\rho}_{sp} > \rho_s > 0$ *satisfy*

$$-\alpha_3(\alpha_2^{-1}(\rho_s)) + (L_x + \sum_{i=1}^{m} L_{\bar{u}_i} \bar{u}_i^{max}) M\Delta + L_w \theta \leq -\varepsilon_w/\Delta. \tag{4.13}$$

and let $\bar{\rho}_{sp}$ *be defined such that if* $x(t_k) \in \Omega_{\bar{\rho}_{sp}}$, *then* $x(t) \in \Omega_{\rho_{sp}} \forall t \in [t_k, t_{k+1})$. *If* $x(t_0) \in \Omega_\rho$, $\rho_{\min} < \rho$ *and* $N \geq 1$, *then the state* $x(t)$ *of the closed-loop system can be driven in a finite time to* $\Omega_{\rho_{sp}}$ *and then be bounded there, and after* t_s *the state* $x(t)$ *of the closed-loop system is ultimately*

bounded in $\Omega_{\rho_{\min}}$ with $\Omega_{\rho_{\min}}$ defined as in Proposition 4.1.

Proof 4.1 *The proof consists of three parts. We first prove that the optimization problem of Eq. 4.8 is recursively feasible for all $x(t_0) \in \Omega_\rho$. Subsequently, we prove that under the Safety-S-DLEMPC design of Eq. 4.8, the closed-loop state of the system of Eq. 4.1 is maintained within Ω_ρ at all times (i.e., Ω_ρ is a forward invariant set), and is driven in finite time into $\Omega_{\rho_{sp}}$ and thereafter bounded there. Finally, we prove that after t_s, the closed-loop state under the Safety-S-DLEMPC of Eq. 4.8 is ultimately bounded in $\Omega_{\rho_{\min}}$.*

Part 1: The feasibility of the optimization problem for Safety-S-DLEMPC j (for $j = 1,\ldots,m$) when $x(t_0) \in \Omega_\rho$ follows because the solution $K_c(t) = 0,\ \forall\, t \in [t_k, t_{k+N})$, $\bar{u}_j(t) = \bar{h}_j(\tilde{x}^j(t_n)),\ \forall\, t \in [t_n, t_{n+1})$, with $n = k,\ldots,N+k-1$, is a feasible solution both when K_c is pre-set to zero throughout the prediction horizon and when it is not. The gain $K_c(t) = 0,\ \forall\, t \in [t_k, t_{k+N})$, is feasible since it satisfies Eq. 4.8g over the prediction horizon. When $K_c(t) = 0$, then by Eq. 4.8i, $\tilde{\rho}(t)$ will be equal to its initial value throughout the prediction horizon, and thus the upper bound on the Lyapunov function in Eq. 4.8h will be fixed (i.e., either $\tilde{\rho}(t_k) = V(x(t_k)) \Rightarrow V(\tilde{x}^j(t)) \leq V(x(t_k)),\ \forall\, t \in [t_k, t_{k+N}),$ if $x(t_k) \notin \Omega_{\rho_{sp}}$ or $\tilde{\rho}(t_k) = \rho_{sp} \Rightarrow V(\tilde{x}^j(t)) \leq \rho_{sp},\ \forall\, t \in [t_k, t_{k+N}),$ if $x(t_k) \in \Omega_{\rho_{sp}}$). In such a case, $\bar{u}_j(t) = \bar{h}_j(\tilde{x}^j(t_n)),\ \forall\, t \in [t_n, t_{n+1})$, with $n = k,\ldots,N+k-1$, satisfies the input constraint of Eq. 4.8c. To prove that $\bar{u}_j(t) = \bar{h}_j(\tilde{x}^j(t_n)),\ \forall\, t \in [t_n, t_{n+1})$, $n = k,\ldots,N+k-1$, satisfies Eqs. 4.8h and 4.8j and is thus a feasible solution to Safety-S-DLEMPC j when $\bar{u}_r(t) = \bar{h}_r(\tilde{x}^j(t_{k+q}))$, $r = j+1,\ldots,m$, $\forall\, t \in [t_{k+q}, t_{k+q+1})$, $q = 0,\ldots,N-1$, and $\bar{u}_p(t) = \bar{u}_p^*(t|t_k)$, $p = 1,\ldots,j-1$, $\forall\, t \in [t_k, t_{k+N})$, as required by Eqs. 4.8d and 4.8e, the sequence of distributed controllers must be evaluated. We will proceed by induction. When $j = 1$, $\bar{u}_j(t) = \bar{h}_j(\tilde{x}^j(t_n)),\ \forall\ t \in [t_n, t_{n+1})$, $n = k,\ldots,N+k-1$, satisfies Eq. 4.8h in Safety-S-DLEMPC 1 by Proposition 4.1 when $x(t) \in \Omega_\rho$, and trivially satisfies the constraint of Eq. 4.8j since $\bar{u}_r(t)$, $r = 2,\ldots,m$ are set to $\bar{h}_r(\tilde{x}^j)$ implemented in sample-and-hold through Eq. 4.8e. Thus, $K_c(t) = 0,\ \forall\, t \in [t_k, t_{k+N})$, $\bar{u}_j(t) = \bar{h}_j(\tilde{x}^j(t_n)),\ \forall\, t \in [t_n, t_{n+1})$, $n = k,\ldots,N+k-1$, is a feasible solution for Safety-S-DLEMPC 1.

Now, assume that there exists a feasible solution to Safety-S-DLEMPC $j-1$ (i.e., $\bar{u}_p^*(t|t_k)$, $p = 1,\ldots,j-1,\ \forall\ t \in [t_k, t_{k+N})$) and that feasibility of $\bar{u}_j(t) = \bar{h}_j(\tilde{x}^j(t_n)),\ \forall\, t \in [t_n, t_{n+1})$, $n =$

$k,\ldots,N+k-1$, *is being considered for Safety-S-DLEMPC* j. *Because Safety-S-DLEMPC* $j-1$ *was feasible (i.e., Eqs. 4.8h and 4.8j were satisfied) when* $\bar{u}_p(t) = \bar{u}_p^*(t|t_k)$, $p = 1,\ldots,j-1$, $\forall\, t \in [t_k, t_{k+N})$, *with all other inputs set to the corresponding components of* $\bar{h}(x)$ *implemented in sample-and-hold, the same input trajectory (i.e.,* $\bar{u}_j(t) = \bar{h}_j(\tilde{x}^j(t_n))$, $\forall\, t \in [t_n, t_{n+1})$, $n = k,\ldots,N+k-1$, *and the other inputs defined according to Eqs. 4.8d and 4.8e) will be feasible for Safety-S-DLEMPC* j *because it will again satisfy Eqs. 4.8h and 4.8j; the feasibility of this solution is independent of the value of* K_c *in Safety-S-DLEMPC* $j-1$ *or Safety-S-DLEMPC* j. *Therefore,* $K_c(t) = 0,\ \forall\, t \in [t_k, t_{k+N})$, $\bar{u}_j(t) = \bar{h}_j(\tilde{x}^j(t_n)),\ \forall\, t \in [t_n, t_{n+1})$, $n = k,\ldots,N+k-1$, *is a feasible solution for Safety-S-DLEMPC 1 and also for Safety-S-DLEMPC* j *when Safety-S-DLEMPC* $j-1$ *is feasible; by induction,* $K_c(t) = 0, \forall\, t \in [t_k, t_{k+N})$, $\bar{u}_j(t) = \bar{h}_j(\tilde{x}^j(t_n)),\ \forall\, t \in [t_n, t_{n+1})$, $n = k,\ldots,N+k-1$, *is therefore a feasible control action for each Safety-S-DLEMPC* j, $j = 1,\ldots,m$. *Recursive feasibility of the Safety-S-DLEMPC follows if the closed-loop state trajectory is maintained within* Ω_ρ *(which will be proven in Part 2 to hold for all times if* $x(t_0) \in \Omega_\rho$*).*

Part 2: We now prove that if $x(t_k)$ *is initialized outside the safety level set (i.e.,* $x(t_k) \in \Omega_\rho / \Omega_{\rho_{sp}}$ *and* $t_k \leq t_s$*), then the closed-loop state remains bounded within* Ω_ρ *(i.e.,* $x(t) \in \Omega_\rho$ *when* $x(t_0) \in \Omega_\rho$*) and within finite time, the closed-loop state will be driven to* $\Omega_{\rho_{sp}}$ *and remain there for all subsequent times under the Safety-S-DLEMPC design of Eq. 4.8.*

Due to the sequential solution strategy of the Safety-S-DLEMPC architecture, the set of control actions $u_j^*(t_k|t_k)$, $j = 1,\ldots,m$, *that are implemented on the process (and thus affect closed-loop stability) satisfy the constraints of the Safety-S-DLEMPC of Eq. 4.8 when* $j = m$. *When* $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$, *from the constraint of Eq. 4.8j of the Safety-S-DLEMPC m of Eq. 4.8 and from Eq. 4.2b, we obtain:*

$$\frac{\partial V(x(t_k))}{\partial x}(f(x(t_k)) + \sum_{i=1}^{m} g_i(x(t_k))\bar{u}_i^*(t_k|t_k)) \leq \frac{\partial V(x(t_k))}{\partial x}(f(x(t_k)) + \sum_{i=1}^{m} g_i(x(t_k))\bar{h}_i(x(t_k))) \tag{4.14a}$$

$$\leq -\alpha_3(|x(t_k)|) \tag{4.14b}$$

The time derivative of the Lyapunov function along the actual system state trajectory $x(t)$ for $t \in [t_k, t_{k+1})$ can be written as follows:

$$\dot{V}(x(t)) = \frac{\partial V(x(t))}{\partial x}\left(f(x(t)) + \sum_{i=1}^{m} g_i(x(t))\bar{u}_i^*(t_k|t_k) + b(x(t))w(t) \right) \tag{4.15}$$

Adding and subtracting $\frac{\partial V(x(t_k))}{\partial x}(f(x(t_k)) + \sum_{i=1}^{m} g_i(x(t_k))\bar{u}_i^*(t_k|t_k))$ *to/from the above equation and accounting for Eq. 4.14, the bound on the disturbance ($|w| \leq \theta$), and the Lipschitz properties of Eqs. 4.4-4.6, we can write:*

$$\dot{V}(x(t)) \leq -\alpha_3(|x(t_k)|) + \left(L_x + \sum_{i=1}^{m} L_{\bar{u}_i}\bar{u}_i^*(t_k|t_k) \right)|x(t) - x(t_k)| + L_w\theta \tag{4.16}$$

From Eq. 4.3 and the continuity of $x(t)$, the following bound can be written for all $t \in [t_k, t_{k+1})$:

$$|x(t) - x(t_k)| \leq M\Delta \tag{4.17}$$

Since $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$, it can be concluded that $x(t_k) \in \Omega_\rho / \Omega_{\rho_s}$. Using this, as well as Eqs. 4.16-4.17 and the bounds on the inputs $\bar{u}_i,\ i = 1, \ldots, m$, we obtain the following bound on $\dot{V}(x(t))$ for $t \in [t_k, t_{k+1})$:

$$\dot{V}(x(t)) \leq -\alpha_3(\alpha_2^{-1}(\rho_s)) + \left(L_x + \sum_{i=1}^{m} L_{\bar{u}_i}\bar{u}_i^{max} \right) M\Delta + L_w\theta \tag{4.18}$$

If the condition of Eq. 4.13 is satisfied, then there exists $\varepsilon_w > 0$ such that the following inequality holds for $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$:

$$\dot{V}(x(t)) \leq -\varepsilon_w/\Delta \quad \forall\, t \in [t_k, t_{k+1}) \tag{4.19}$$

Integrating the bound of Eq. 4.19 on $t \in [t_k, t_{k+1})$ we obtain that:

$$V(x(t_{k+1})) \leq V(x(t_k)) - \varepsilon_w \tag{4.20a}$$

$$V(x(t)) \leq V(x(t_k)), \ \ \forall\, t \in [t_k, t_{k+1}) \tag{4.20b}$$

for all $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$. Using Eq. 4.20 recursively, it is proved that, if $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$, the state converges to $\Omega_{\bar{\rho}_{sp}}$ in a finite number of sampling times while remaining within Ω_ρ throughout the transition since $V(x)$ does not increase. Once the state converges to $\Omega_{\bar{\rho}_{sp}} \subseteq \Omega_{\rho_{sp}}$, it remains inside $\Omega_{\rho_{sp}}$ for all times from the definition of $\Omega_{\bar{\rho}_{sp}}$ in Theorem 4.1 (i.e., if $x(t_k) \in \Omega_{\bar{\rho}_{sp}}$, then $x(t) \in \Omega_{\rho_{sp}} \forall t \in [t_k, t_{k+1})$) and re-activation of the contractive constraint of Eq. 4.8j to decrease the Lyapunov function value until $x(t_k) \in \Omega_{\bar{\rho}_{sp}}$ whenever $x(t_k) \in \Omega_{\rho_{sp}} / \Omega_{\bar{\rho}_{sp}}$. Since $\Omega_{\rho_{sp}} \subseteq \Omega_\rho$, the state of the closed-loop system is always maintained within Ω_ρ making it a forward invariant set.

Part 3: Finally, we prove ultimate boundedness of the closed-loop state within $\Omega_{\rho_{\min}}$ when $t_k > t_s$. If $t_k > t_s$, then Eq. 4.8j is active at all subsequent sampling times. Since Eq. 4.19 holds whenever $x(t_k) \in \Omega_\rho / \Omega_{\rho_s}$, Eq. 4.20a also holds and thus for $x(t_k) \in \Omega_\rho / \Omega_{\rho_s}$, $V(x(t_{k+1})) < V(x(t_k))$ and the closed-loop state moves to lower level sets until $x(t_k) \in \Omega_{\rho_s}$. From the definition of $\Omega_{\rho_{\min}}$ in Proposition 4.1, once the state converges to $\Omega_{\rho_s} \subseteq \Omega_{\rho_{\min}}$, it remains inside $\Omega_{\rho_{\min}}$ for all times.

Remark 4.3 *The definition of $\Omega_{\bar{\rho}_{sp}}$ in Theorem 4.1 removes the direct correspondence between a constraint of the form in Eq. 4.8h and the proof of closed-loop stability that is made in other works on LEMPC (e.g.,[43]). To determine $\bar{\rho}_{sp}$, closed-loop simulations could be performed utilizing worst-case scenarios for the process model of Eq. 4.1 based on bounds on the disturbances and inputs in calculating the value of $\Omega_{\bar{\rho}_{sp}}$. In such a case, the constraint of Eq. 4.8h would not play a role in the closed-loop stability proof. An alternative implementation of the Safety-S-DLEMPC strategy would, however, allow a bound on $\bar{\rho}_{sp}$ to be determined based on satisfaction of a constraint of the form of Eq. 4.8h. Specifically, because the primary purpose of the constraint of Eq. 4.8h is in driving the closed-loop state to the safety region, once the closed-loop state enters the safety region, it is no longer necessary to utilize the safety-based constraints. Therefore, Eqs. 4.8g-4.8j can be*

replaced by the standard Mode 1 and Mode 2 constraints of[43] *once the closed-loop state enters* $\Omega_{\rho_{sp}}$ *(and the penalty term in the objective function could be removed). The Mode 1 constraint would be the constraint of Eq. 4.8h but with the upper bound on the Lyapunov function fixed to* $\bar{\rho}_{sp}$*, and the activation condition being that* $x(t_k) \in \Omega_{\bar{\rho}_{sp}}$*. The Mode 2 constraint would be the constraint of Eq. 4.8j. With this modification, an explicit bound can be utilized on* $\bar{\rho}_{sp}$ *to prove that the closed-loop state is maintained within* $\Omega_{\rho_{sp}}$ *for all times after this region is entered, where the bound is based on satisfaction of the Mode 1 constraint requiring* $V(\tilde{x}^j) \leq \bar{\rho}_{sp}$ *when* $x(t_k) \in \Omega_{\bar{\rho}_{sp}}$*.*

Remark 4.4 *The focus of this chapter is on distributed safety-based LEMPC designs; however, a safety-based tracking Lyapunov-based model predictive control (LMPC) design presented in Chapter 3 which takes the form of the centralized safety-based LEMPC design in Eq. 4.7 but with the contractive constraint of Eq. 4.7h enforced for all times, regardless of the location in state-space of the measurement of the state at* t_k*. Due to the similarity of this design to the centralized safety-based LEMPC design considered in this chapter, the results in this chapter, including the closed-loop stability and feasibility results, can be readily extended to the LMPC design considered in that work. For the sequential design, the same architecture and implementation strategy can be employed, with a similar formulation for the* $j-th$ *distributed controller as in Eq. 4.8 but with the contractive constraint always activated,* K_c *can be set to zero in some of the distributed controllers and inputs can be grouped based on their effect on* $V(\tilde{x})$*, and the results of Theorem 4.1 would hold for the resulting formulation, effectively with* $t_s = t_0$ *due to the repeated application of the contractive constraint.*

4.3.2 Safety-Iterative-DLEMPC

An alternative to the Safety-S-DLEMPC that may in some cases demonstrate improved performance compared to the Safety-S-DLEMPC (i.e., the implemented control actions may minimize the objective function more significantly) is a Safety-Iterative-DLEMPC (Safety-I-DLEMPC). As for the Safety-S-DLEMPC, there are m controllers, but unlike for the Safety-S-DLEMPC, all m controllers are solved simultaneously. In addition, the constraint of Eq. 4.8j in the j^{th} Safety-S-

DLEMPC, $j = 1,\ldots,m$, is reformulated. The first time that the m controllers are solved, the j^{th} controller (Safety-I-DLEMPC j) solves for $\bar{u}_j$ and K_c and assumes that $\bar{u}_z(t)$, $z \in \{1,\ldots,m\}$ but $z \neq j$, are equal to $\bar{h}_z(\tilde{x}^j(t_q))$, $\forall\, t \in [t_q, t_{q+1})$, $q = k,\ldots,k+N-1$. After the solutions of all m controllers have been obtained, the Safety-I-DLEMPC can cause the solutions of these m controllers to be implemented, or they can be exchanged. If the solutions are exchanged, each of the Safety-I-DLEMPC's is re-solved for $\bar{u}_j$ and K_c assuming that $\bar{u}_z$, $z \in \{1,\ldots,m\}$ but $z \neq j$, are equal to the trajectories of $\bar{u}_z$ returned by each of the m controllers at the prior iteration. In general, the number of iterations is an integer $c \in [1,\infty)$. When it is necessary to clearly specify the iteration number associated with the solution of the Safety-I-DLEMPC's below, we will refer to the solution to Safety-I-DLEMPC j at time t_k at iteration c as $\bar{u}^*_{j,c}(t|t_k)$ and $K_{c,c}(t|t_k)$, $\forall\, t \in [t_k, t_{k+N})$. Termination of the exchange of solutions (i.e., preventing further iterations at a given time t_k) can be triggered by various conditions. Examples of considerations that could be used are a fixed number of iterations or terminating when the value of the objective function evaluated for the predicted state of the nominal process under the inputs calculated by the m Safety-I-DLEMPC's at iteration c is no better than the cost function at iteration $c-1$ or is better by no more than a termination condition ε.

The proposed formulation of Safety-I-DLEMPC $j,\ j = 1,\ldots,m$, at iteration c is as follows:

$$\max_{\bar{u}_j, K_c \in S(\Delta)} \int_{t_k}^{t_{k+N}} [L_e(\tilde{x}^j(\tau), \bar{u}_1(\tau), \ldots, \bar{u}_m(\tau)) - \tag{4.21a}$$

$$\phi(\rho_{sp} - \tilde{\rho}(\tau))] d\tau$$

$$\text{s.t. } \dot{\tilde{x}}^j(t) = f(\tilde{x}^j(t)) + \sum_{i=1}^{m} g_i(\tilde{x}^j(t))\bar{u}_i(t) \tag{4.21b}$$

$$\bar{u}_j(t) \in U_j,\ \forall\, t \in [t_k, t_{k+N}) \tag{4.21c}$$

$$\bar{u}_z(t) = \bar{u}^*_{z,c-1}(t|t_k),\ z \in \{1,\ldots,m\},\ z \neq j,\ \forall\, t \in [t_{k+r}, t_{k+r+1}),$$

$$r = 0,\ldots,N-1,\ c \geq 2 \tag{4.21d}$$

$$\bar{u}_z(t) = \bar{h}_z(\tilde{x}^j(t_{k+r})),\ z \in \{1,\ldots,m\},\ z \neq j,\ \forall\, t \in [t_{k+r}, t_{k+r+1}),$$

$$r = 0,\ldots,N-1,\ c = 1 \tag{4.21e}$$

$$\tilde{x}^j(t_k) = x(t_k) \tag{4.21f}$$

$$K_c(t) \geq 0,\ \forall\, t \in [t_k, t_{k+N}) \tag{4.21g}$$

$$V(\tilde{x}^j(t)) \leq \tilde{\rho}(t),\ \forall\, t \in [t_k, t_{k+N}) \tag{4.21h}$$

$$\frac{d\tilde{\rho}}{dt} = K_c(t)(\rho_{sp} - \tilde{\rho}(t)) \tag{4.21i}$$

$$\tilde{\rho}(t_k) = V(x(t_k)), \quad \text{if } x(t_k) \notin \Omega_{\rho_{sp}}$$

$$\tilde{\rho}(t_k) = \rho_{sp}, \quad \text{if } x(t_k) \in \Omega_{\rho_{sp}}$$

$$\frac{\partial V(x(t_k))}{\partial x} g_j(x(t_k))\bar{u}_j(t_k) \tag{4.21j}$$

$$\leq \frac{\partial V(x(t_k))}{\partial x} g_j(x(t_k))\bar{h}_j(x(t_k)),$$

$$\text{if } x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}} \text{ or } t_k > t_s$$

where as for the Safety-S-DLEMPC, K_c may be set to zero in any of the m Safety-I-DLEMPC's as desired. The constraint of Eq. 4.21d sets the input trajectories $\bar{u}_z(t)$, $z \in \{1,\ldots,m\}$ where $z \neq j$, to their optimal solution in the previous iteration assuming $c > 1$, whereas the constraint of Eq. 4.21e sets the input trajectories to the corresponding Lyapunov-based control laws imple-

mented in sample-and-hold when there is no prior iteration (i.e., $c = 1$). The notation of the other constraints follows that in Eq. 4.8.

The implementation strategy for the Safety-I-DLEMPC architecture is as follows:

1. At t_k, all m Safety-I-DLEMPC's receive a measurement of the current state $x(t_k)$ from the sensors. Go to Step 2.

2. At iteration c ($c \geq 1$):

   (a) If $c = 1$, Safety-I-DLEMPC j assumes $\bar{u}_z(t) = \bar{h}_z(\tilde{x}^j(t_{k+q}))$, $\forall\ t \in [t_{k+q}, t_{k+q+1})$, $z \in \{1,\ldots,m\}$ but $z \neq j$, $q = 0,\ldots,N-1$. If $c > 1$, Safety-I-DLEMPC j assumes $\bar{u}_z(t) = \bar{u}^*_{z,c-1}(t|t_k)$, $\forall\ t \in [t_{k+r}, t_{k+r+1})$, $r = 0,\ldots,N-1$, $z \in \{1,\ldots,m\}$ but $z \neq j$. Using these values, Safety-I-DLEMPC j evaluates both the optimal input trajectory $\bar{u}^*_{j,c}(\tau|t_k)$, and the optimal gain $K^*_{c,c}(\tau|t_k)$, $\tau \in [t_k, t_{k+N})$, or only the optimal input trajectory $\bar{u}^*_{j,c}(\tau|t_k)$, $\forall\ \tau \in [t_k, t_{k+N})$, when Safety-I-DLEMPC j sets the value of the gain K_c to zero. Go to Step 2b.

   (b) Both the constraint of Eq. 4.21h under $\bar{u}^*_{j,c}(\tau|t_k)$, $\forall\ \tau \in [t_k, t_{k+N})$, where $j = 1,\ldots,m$ (i.e., $V(\tilde{x}^{tot}) \leq V(x(t_k))$, $\forall\ t \in [t_k, t_{k+N})$, if $x(t_k) \notin \Omega_{\rho_{sp}}$, or $V(\tilde{x}^{tot}(t)) \leq \rho_{sp}$, $\forall\ t \in [t_k, t_{k+N})$, if $x(t_k) \in \Omega_{\rho_{sp}}$, where $\tilde{x}^{tot}$ is the predicted state trajectory of the nominal system of Eq. 4.1 under $\bar{u}^*_{j,c}(\tau|t_k)$, $\forall\ \tau \in [t_k, t_{k+N})$, $j = 1,\ldots,m$) and the iteration termination condition are evaluated. If Eq. 4.21h is not met or the iteration termination condition is met, go to Step 2c. Else, go to Step 2d.

   (c) If $c > 1$, implement $[\bar{u}^*_1(t_k|t_k)\ \ldots\ \bar{u}^*_m(t_k|t_k)] = [\bar{u}^*_{1,c-1}(t_k|t_k)\ \ldots\ \bar{u}^*_{m,c-1}(t_k|t_k)]$. Else, implement $[\bar{u}^*_1(t_k|t_k)\ \ldots\ \bar{u}^*_m(t_k|t_k)] = [\bar{h}_1(x(t_k))\ \ldots\ \bar{h}_m(x(t_k))]$. Go to Step 3.

   (d) The optimal input trajectories are exchanged between the Safety-I-DLEMPC controllers. The controller stores any required values related to the iteration termination condition (e.g., the calculated value of the objective function used in evaluating the iteration termination condition). Go to Step 2a ($c \leftarrow c + 1$).

3. When a new state measurement is received at t_{k+1}, go to Step 1 ($k \leftarrow k+1$).

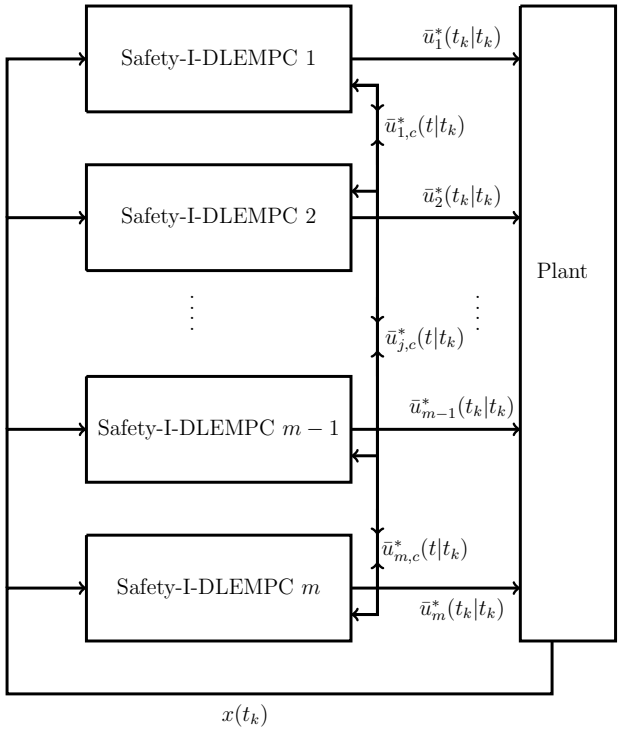

Figure 4.2: Block diagram of the Safety-I-DLEMPC scheme

A schematic of the Safety-I-DLEMPC scheme is shown in Figure 4.2. At iteration c, Safety-I-DLEMPC j calculates the optimal solution $\bar{u}_{j,c}^*(t|t_k)$, $\forall\ t \in [t_k, t_{k+N})$, with the piecewise-constant gain $K_{c,c}^*(\tau|t_k)$, $\tau \in [t_k, t_{k+N})$, corresponding to that iteration. The values of $\bar{u}_1, \ldots, \bar{u}_m$ that are implemented on the process throughout the sampling period from t_k to t_{k+1} as a result of the above implementation strategy for the Safety-I-DLEMPC architecture are denoted by $u_1^*(t_k|t_k), \ldots, u_m^*(t_k|t_k)$.

As for the Safety-S-DLEMPC architecture, the number of controllers in which to solve for K_c and the method of partitioning the inputs into vectors $\bar{u}_1$, $\bar{u}_2$, and so on are important considerations, which rely on the above implementation strategy for the Safety-I-DLEMPC. It is noted that because the m Safety-I-DLEMPC's are solved independently, assuming in each controller different values of $\bar{u}_z$, $z \in \{1, \ldots, m\}$ but $z \neq j$, than are used by the other controllers, there is no guarantee that the constraint of Eq. 4.21h is satisfied for the nominal system of Eq. 4.1 under the set of trajectories $\bar{u}_{1,c}^*, (t|t_k) \ldots, \bar{u}_{m,c}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, returned by the set of Safety-I-DLEMPC's

at iteration c, even if $K_c = 0$ in Eq. 4.21h. However, satisfaction of Eq. 4.21h by this trajectory would be required for proving feasibility of the next iteration for the Safety-I-DLEMPC design. Therefore, it is necessary to check whether Eq. 4.21h is satisfied by the optimal control actions at the end of every iteration (i.e., compute the solution $\tilde{x}^{tot}$ to the nominal system of Eq. 4.1 under $\bar{u}^*_{1,c}(t|t_k),\ldots,\bar{u}^*_{m,c}(t|t_k)$, $\forall\, t \in [t_k, t_{k+N})$, and check whether $V(\tilde{x}^{tot}) \leq V(x(t_k))$ if $x(t_k) \in \Omega_\rho/\Omega_{\rho_{sp}}$ or $V(\tilde{x}^{tot}) \leq \rho_{sp}$ if $x(t_k) \in \Omega_{\rho_{sp}}$ throughout the prediction horizon). If this condition is satisfied, then the solution $\bar{u}^*_{1,c}(t|t_k),\ldots,\bar{u}^*_{m,c}(t|t_k)$, $\forall\, t \in [t_k, t_{k+N})$, at iteration c can be implemented or exchanged between the controllers and another iteration can begin. If Eq. 4.21h is not satisfied, then either the solution from iteration $c-1$ that met the condition should be implemented when $c > 1$, or $\bar{h}(x(t_k))$ should be implemented if $c = 1$. This strategy, which keeps the optimization problem of Eq. 4.21 feasible at each sampling time t_k, has been included in the above implementation strategy.

To determine whether K_c can be set to zero in some of the Safety-I-DLEMPC's given this implementation strategy, without negatively impacting closed-loop stability, to decrease the number of optimization variables in some of the Safety-I-DLEMPC's, we appeal to feasibility and closed-loop stability arguments. First, consider iteration $c = 1$. In this case, the j^{th} Safety-I-DLEMPC assumes that $\bar{u}_z(t)$, $z \in \{1,\ldots,m\}$ but $z \neq j$, is equal to $\bar{h}_z(x(t_q))$, $q = k,\ldots,k+N-1$, $\forall\, t \in [t_k, t_{k+N})$, and solves for $\bar{u}_j$ and K_c. The solution $\bar{u}_j(t) = \bar{h}_i(x(t_q))$, $q = k,\ldots,k+N-1$, $\forall\, t \in [t_k, t_{k+N})$, with $K_c = 0$, $\forall\, t \in [t_k, t_{k+1})$, is a feasible solution for the j^{th} Safety-I-DLEMPC; therefore, there is always a feasible solution to all Safety-I-DLEMPC's for $c = 1$. To ensure feasibility of subsequent iterations, there must be a feasible solution to the constraint of Eq. 4.21h at the next iteration. This is ensured, regardless of whether $K_c(t) \equiv 0$, $\forall\, t \in [t_k, t_{k+N})$, if $V(\tilde{x}^{tot})$ is below a required bound throughout the prediction horizon at the prior iteration. The LEMPC implementation strategy ensures that no subsequent iterations are performed if this iteration condition is not met; therefore, all attempted iterations will have a feasible solution, regardless of whether $K_c(t) \equiv 0$, $\forall\, t \in [t_k, t_{k+N})$, under the Safety-I-DLEMPC implementation strategy. It is important to ensure that a control action implemented by the Safety-I-DLEMPC implementation strategy will be stabilizing (i.e., $x(t) \in \Omega_\rho$ for all times, and $x(t)$ enters $\Omega_{\rho_{sp}}$ in finite time and

remains in $\Omega_{\rho_{sp}}$ thereafter). If $\bar{u}^*_{1,c-1}(t_k|t_k),\ldots,\bar{u}^*_{m,c-1}(t|t_k)$, $\forall\ t\in[t_k,t_{k+N})$, is implemented, a summation of the constraints of Eq. 4.21j for all m Safety-I-DLEMPC's reveals that Eq. 4.14a is met by these control actions (and therefore, utilizing similar steps as in the proof of Theorem 4.1, $V(x(t_{k+1}))<V(x(t_k))$). If instead $\bar{h}(x)$ is implemented in sample-and-hold, $V(x(t_{k+1}))<V(x(t_k))$ from Proposition 4.1. If $x(t_k)\in\Omega_{\bar{\rho}_{sp}}$, then under either $u^*_{1,c-1}(t_k|t_k),\ldots,u^*_{m,c-1}(t_k|t_k)$, or $\bar{h}(x)$ implemented in sample-and-hold, $x(t_{k+1})\in\Omega_{\rho_{sp}}$ from the definition of $\Omega_{\bar{\rho}_{sp}}$. This establishes that closed-loop stability is maintained under the Safety-I-DLEMPC implementation strategy because this implementation strategy ensures that the implemented control actions satisfy both Eq. 4.21h and 4.21j. Furthermore, this stability proof does not depend on the value of K_c in each controller, and $K_c=0$, $\forall\ t\in[t_k,t_{k+N})$, is guaranteed to provide a feasible solution to the Safety-I-DLEMPC at $c=1$ and all subsequent attempted iterations. Therefore, it is possible to set K_c to zero in some of the Safety-I-DLEMPC optimization problems to reduce the number of decision variables in these problems. It may be helpful to partition the inputs with a large effect on $V(\tilde{x})$ into some $\bar{u}_j$ vectors and those with more minimal effect into others, so that the Safety-I-DLEMPC's for which solving for $\bar{u}_i$ may have less effect on the safety penalty term can be selected to have $K_c\equiv 0$. However, the effects of partitioning and of setting $K_c\equiv 0$ in some controllers should be assessed with closed-loop simulations.

We will now provide the conditions that guarantee closed-loop stability of a nonlinear process under the Safety-I-DLEMPC implementation strategy, as well as conditions that guarantee feasibility of the Safety-I-DLEMPC optimization problem of Eq. 4.21 at a given iteration.

Theorem 4.2 *Consider the system of Eq. 4.1 in closed-loop under the implementation strategy (steps 1-3) of the iterative distributed safety-based LEMPC design of Eq. 4.21 based on a controller $h(x)$ that satisfies the conditions of Eq. 4.2. Let $\varepsilon_w>0$, $\Delta>0$, $\rho>\rho_{sp}>\bar{\rho}_{sp}>\rho_s>0$ satisfy the constraint of Eq. 4.13, with $\bar{\rho}_{sp}$ defined such that if $x(t_k)\in\Omega_{\bar{\rho}_{sp}}$, then $x(t)\in\Omega_{\rho_{sp}}\forall t\in[t_k,t_{k+1})$. For any $N\geq 1$ and $c\geq 1$, if $x(t_0)\in\Omega_\rho$, $\rho_{\min}<\rho$, then the state $x(t)$ of the closed-loop system can be driven in a finite time to $\Omega_{\rho_{sp}}$ and then be bounded there, and after t_s the state $x(t)$ of the closed-loop system is ultimately bounded in $\Omega_{\rho_{\min}}$ with $\Omega_{\rho_{\min}}$ defined as in Proposition 4.1.*

Proof 4.2 *Like the proof of Theorem 1, the proof of Theorem 2 consists of three parts. We first prove that under steps 1-3 of the safety-I-DLEMPC implementation strategy, the optimization problem of Eq. 4.21 is feasible for each iteration c that is executed when* $x(t_0) \in \Omega_\rho$*, and that the control actions implemented on the process under this implementation strategy have characterizable properties. Then we prove that the closed-loop state of the system of Eq. 4.1 can be driven in finite time into* $\Omega_{\rho_{sp}}$ *under the control actions from the Safety-I-DLEMPC implementation strategy, and then be bounded there. We also prove that under the Safety-I-DLEMPC implementation strategy, the closed-loop state is always maintained in* Ω_ρ *if* $x(t_0) \in \Omega_\rho$ *(i.e.,* Ω_ρ *is a forward invariant set). Finally, we prove that after* t_s*, the closed-loop state under the Safety-I-DLEMPC implementation strategy is ultimately bounded in* $\Omega_{\rho_{\min}}$*.*

Part 1: At the initial iteration (i.e., $c = 1$*) and for all* $x(t_0) \in \Omega_\rho$*, the solution* $K_{c,1}(t) = 0,\ \forall\, t \in [t_k, t_{k+N})$*,* $\bar{u}_{j,1}(t) = \bar{h}_j(\tilde{x}^j(t_n)),\ \forall\, t \in [t_n, t_{n+1})$*, with* $n = k, \ldots, N+k-1$*, is a feasible solution to each Safety-I-DLEMPC* j *of Eq. 4.21,* $j = 1, \ldots, m$*, both when* K_c *is fixed at zero and when it is not. Feasibility of* $K_{c,1}(t) = 0,\ \forall\, t \in [t_k, t_{k+N})$*, at* $c = 1$ *follows because* $K_{c,1}(t) = 0, \forall\, t \in [t_k, t_{k+N})$*, satisfies Eq. 4.21g throughout the prediction horizon. When* $K_{c,1}(t) = 0$*, then as described in the proof of Theorem 4.1, the upper bound on the Lyapunov function in Eq. 4.21h is fixed to either* $V(x(t_k))$ *or* ρ_{sp}*. In such a case,* $\bar{u}_{j,1}(t) = \bar{h}_j(\tilde{x}^j(t_n)),\ \forall\, t \in [t_n, t_{n+1})$*,* $n = k, \ldots, N+k-1$*, satisfies the input constraint of Eq. 4.21c. Because* $\bar{u}_z(t) = \bar{h}_z(\tilde{x}^j(t_{k+r}))$*,* $z \in \{1, \ldots, m\}$*,* $z \neq j$*,* $\forall\, t \in [t_{k+r}, t_{k+r+1})$*,* $r = 0, \ldots, N-1$*, from Eq. 4.21e, the constraint of Eq. 4.21h is satisfied by Proposition 4.1,*[72] *as is the constraint of Eq. 4.21j (trivially). For the subsequent iterations (i.e.,* $c > 1$*), the solution* $K_{c,c}(t) = 0,\ \forall\, t \in [t_k, t_{k+N})$*,* $\bar{u}_{j,c}(t) = \bar{u}^*_{j,c-1}(t|t_k),\ \forall\, t \in [t_n, t_{n+1})$*, with* $n = k, \ldots, N+k-1$*, is a feasible solution to Safety-I-DLEMPC* j*,* $j = 1, \ldots, m$ *(regardless of whether* K_c *is fixed to zero in the optimization problem or not) when the condition of Eq. 4.21h is satisfied by the solutions* $\bar{u}^*_{j,c-1}(t|t_k),\ \forall\, t \in [t_n, t_{n+1}),\ n = k, \ldots, N+k-1,\ j = 1, \ldots, m$*, from the prior iteration, i.e., when* $V(\tilde{x}^{tot}(t)) \leq V(x(t_k)), \forall\, t \in [t_k, t_{k+N})$*, if* $x(t_k) \notin \Omega_{\rho_{sp}}$*, or when* $V(\tilde{x}^{tot}(t)) \leq \rho_{sp}$*,* $\forall\, t \in [t_k, t_{k+N})$*, if* $x(t_k) \in \Omega_{\rho_{sp}}$*, where* $\tilde{x}^{tot}(t),\ \forall\, t \in [t_k, t_{k+N})$*, is defined as the solution obtained by*

recursively solving:

$$\dot{\tilde{x}}^{tot} = f(\tilde{x}^{tot}) + \sum_{i=1}^{m} g_i(\tilde{x}^{tot})\overline{u}^*_{i,c-1}(t|t_k) \tag{4.22}$$

given $\tilde{x}^{tot}(t_k) = x(t_k)$. *Feasibility of this solution follows because since it was feasible at the prior iteration, it satisfied the input constraint of Eq. 4.21c and will also satisfy the constraints of Eqs. 4.21h and 4.21j. Because the upper bound on the Lyapunov function in Eq. 4.21h is the same between two iterations since it is based only on a state measurement at* t_k *and thus will be the same for all iterations at* t_k*, when the condition on* $V(\tilde{x}^{tot}(t))$ *is checked under* $\overline{u}^*_{z,c-1}(t|t_k)$, $z = 1,\ldots,m$, $\forall\ t \in [t_k, t_{k+N})$, *at the end of the prior iteration and now* $\overline{u}_z(t) = \overline{u}^*_{z,c-1}(t|t_k)$, $z \in \{1,\ldots,m\}$, *but* $z \neq j$, $\forall\ t \in [t_k, t_{k+N})$, *within Safety-I-DLEMPC* j *from the constraint of Eq. 4.21d, it is already known from the check at the prior iteration that with those trajectories for all* $\overline{u}_z(t)$ *for* $z \neq j$ *that* $\overline{u}^*_{j,c-1}(t|t_k)$, $\forall\ t \in [t_k, t_{k+N})$, *will meet the constraint of Eq. 4.21h. Finally, unlike the constraint of Eq. 4.21h, the contractive constraint of Eq. 4.21j does not depend on control actions* $\overline{u}_z(t)$, $z \neq j$*; therefore, the solution* $\overline{u}^*_{j,c-1}(t)$ *will satisfy the contractive constraint of Safety-I-DLEMPC* j, *where* $j = 1,\ldots,m$, *at iteration c if it is satisfied at the prior iteration. If the termination condition is met or the condition on* $V(\tilde{x}^{tot}(t))$ *under* $\overline{u}^*_{j,c}(t|t_k)$, $\forall\ t \in [t_k, t_{k+N})$, $j = 1,\ldots,m$, *is not satisfied and* $c > 1$, *then a new iteration is not performed. When the new iteration is not performed, a solution that was feasible at the prior iteration (i.e.,* $\overline{u}^*_{z,c-1}(t|t_k)$, $t \in [t_k, t_{k+N})$, $z = 1,\ldots,m$*) is implemented. Because this solution was feasible for all* j *Safety-I-DLEMPC's,* $j = 1,\ldots,m$, *at the prior iteration, it is known to have satisfied the constraint of each Safety-I-DLEMPC and therefore has characterizable properties. If* $c = 1$ *and the condition on* $V(\tilde{x}^{tot}(t))$ *is not satisfied,* $\overline{h}(x)$ *is implemented in sample-and-hold, which also has characterizable properties (e.g., Proposition 4.1). Therefore, feasibility of the Safety-I-DLEMPC is ensured at each iteration that is attempted due to checking of the condition on* $V(\tilde{x}^{tot}(t))$ *before attempting a new iteration. However, there is no guarantee that this condition will be met at the end of any iteration. When it is not met and iterating stops, however, the solution applied under the implementation strategy (i.e., either* $\overline{u}^*_{j,c-1}(t_k|t_k)$, $j = 1,\ldots,m$, *or* $\overline{h}(x(t_k))$*) has characterizable properties.*

Part 2: We now utilize the known properties of the implemented control actions under the

Safety-I-DLEMPC implementation strategy to prove closed-loop stability of a nonlinear process under this implementation strategy in the sense of boundedness of the closed-loop state. First, we prove that if $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$ *then* $V(x(t_{k+1})) < V(x(t_k))$ *and in finite steps, the closed-loop state converges to* $\Omega_{\bar{\rho}_{sp}}$ *(i.e.,* $x(t_{k+p}) \in \Omega_{\bar{\rho}_{sp}}$ *where* p *is a finite positive integer) in a manner that maintains the closed-loop state within* Ω_ρ*. We then demonstrate that once the closed-loop state enters* $\Omega_{\rho_{sp}}$*, it is bounded there for all subsequent times.*

When $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$ *and* $\overline{u}^*_{j,c-1}(t_k|t_k)$*,* $j = 1, \ldots, m$*, is applied to the plant, Eq. 4.21j holds for each implemented control action. By summing the constraints of Eq. 4.21j for all* j *Safety-I-DLEMPC's,* $j = 1, \ldots, m$*, and utilizing Eq. 4.2b, we obtain:*

$$\sum_{j=1}^{m} \frac{\partial V(x(t_k))}{\partial x} g_j(x(t_k)) \overline{u}^*_{j,c-1}(t_k|t_k) \leq \sum_{j=1}^{m} \frac{\partial V(x(t_k))}{\partial x} g_j(x(t_k)) \bar{h}_j(x(t_k)) \tag{4.23a}$$

$$= \frac{\partial V(x(t_k))}{\partial x} \left(f(x(t_k)) + \sum_{j=1}^{m} g_j(x(t_k)) \overline{u}^*_{j,c-1}(t_k|t_k) \right) \leq \frac{\partial V(x(t_k))}{\partial x} \left(f(x(t_k)) + \sum_{j=1}^{m} g_j(x(t_k)) \bar{h}_j(x(t_k)) \right) \tag{4.23b}$$

$$\leq -\alpha_3(|x(t_k)|) \tag{4.23c}$$

Following the same approach as in the proof of Theorem 1, if the condition of Eq. 4.13 is satisfied, then $V(x(t_{k+1})) < V(x(t_k))$ *under the implemented control action. If* $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$ *but* $\bar{h}(x(t_k))$ *is applied to the plant, then by Proposition 4.1,* $V(x(t_{k+1})) < V(x(t_k))$*. Therefore, at any given sampling time when* $x(t_k) \in \Omega_\rho / \Omega_{\bar{\rho}_{sp}}$*, regardless of whether* $\overline{u}^*_{j,c-1}(t_k|t_k)$*,* $i = 1, \ldots, m$*, or* $\bar{h}(x(t_k))$ *is implemented according to the implementation strategy of the Safety-I-DLEMPC,* $V(x(t_{k+1})) < V(x(t_k))$ *and this will cause the closed-loop state to be driven into* $\Omega_{\bar{\rho}_{sp}}$ *in finite time in a manner that cannot exit* Ω_ρ*. When* $\Omega_{\bar{\rho}_{sp}}$ *is defined as in Theorem 4.2 such that if* $x(t_k) \in \Omega_{\bar{\rho}_{sp}}$*, then* $x(t) \in \Omega_{\rho_{sp}} \forall t \in [t_k, t_{k+1})$*, the result is that* $\Omega_{\rho_{sp}}$ *is a forward invariant set. This is because if* $x(t_k) \in \Omega_{\rho_{sp}} / \Omega_{\bar{\rho}_{sp}}$*, the constraint of Eq. 4.21j is active when computing the* $\overline{u}^*_{j,c-1}(t_k|t_k)$*,* $j = 1, \ldots, m$*, that are applied to the plant, and thus either a solution that meets that constraint or* $\bar{h}(x(t_k))$ *will be applied to the plant. The result will be that* $V(x(t_{k+1})) < V(x(t_k))$*, so if* $x(t_k) \in \Omega_{\rho_{sp}} / \Omega_{\bar{\rho}_{sp}}$*, then*

$x(t_{k+1}) \in \Omega_{\rho_{sp}}$. *If* $x(t_k) \in \Omega_{\bar{\rho}_{sp}}$, *then* $x(t_{k+1}) \in \Omega_{\rho_{sp}}$ *from the definition of* $\Omega_{\bar{\rho}_{sp}}$. *Therefore, once the closed-loop state enters* $\Omega_{\rho_{sp}}$ *under this implementation strategy, it cannot leave it. Furthermore, since* $\Omega_{\rho_{sp}} \subseteq \Omega_{\rho}$, *the closed-loop state under this implementation strategy is always bounded in* Ω_{ρ}.

Part 3: When $t_k > t_s$, *either inputs* $\bar{u}^*_{j,c-1}(t_k|t_k)$, $j = 1,\ldots,m$, *that cause Eq. 4.23 to hold are applied to the plant, or the Lyapunov-based controller implemented in sample-and-hold is applied, for which the results of Proposition 4.1 hold. Following similar steps as in the proof of Part 3 of Theorem 1, this causes* $V(x(t_{k+1})) \leq V(x(t_k))$ *while* $x(t_k) \in \Omega_{\rho}/\Omega_{\rho_s}$, *driving the closed-loop state into* Ω_{ρ_s} *in finite time. Subsequently, from the definition of* $\Omega_{\rho_{\min}}$, *the system state is ultimately bounded in an invariant set* $\Omega_{\rho_{\min}}$ *under the implementation strategy of the Safety-I-DLEMPC.*

Remark 4.5 *For the proof of closed-loop stability and feasibility of the Safety-I-DLEMPC design, similar comments as in Remark 4.3 can be made. Firstly, the constraint of Eq. 4.21h is not utilized in the proof of closed-loop stability. Also, once the closed-loop state enters the safety region, the Safety-I-DLEMPC can be modified to no longer include the penalty term in the objective function or safety-based constraints, but can instead by formulated like an iterative distributed LEMPC with the constraints of Eqs. 4.21g-4.21i replaced by the constraint of Eq. 4.21h but with a static upper bound of* $\bar{\rho}_{sp}$ *on the Lyapunov function, and the constraint activated whenever the closed-loop state is within* $\Omega_{\bar{\rho}_{sp}}$. *The same implementation strategy could continue to be used after this modification (e.g., checking the value of* $V(\tilde{x}^{tot}(t))$ *between iterations). This discussion brings up two important points regarding the Safety-I-DLEMPC closed-loop stability and feasibility proof:*

1. *Though satisfaction of the condition on* $V(\tilde{x}^{tot}(t))$ *is not directly utilized for proving closed-loop stability, checking the condition on* $V(\tilde{x}^{tot}(t))$ *was shown through the proof of feasibility to be important in ensuring that there was a feasible solution to Safety-I-DLEMPC* j, $j = 1,\ldots,m$, *at each iteration attempted.*

2. *Because only the slight modifications discussed in this remark to Eqs. 4.21a and 4.21g-4.21i are required to transform the Safety-I-DLEMPC into an iterative distributed LEMPC (i.e.,*

not including safety-based constraints), the implementation strategy proposed above with the resulting guarantees on closed-loop stability within $\Omega_{\rho_{sp}}$ and feasibility of the optimization problem at every sampling time for $c = 1$ and at subsequent sampling times when the condition on $V(\tilde{x}^{tot}(t))$ is met would also hold. This is significant because it is the first closed-loop stability result for iterative distributed LEMPC in general.

Remark 4.6 *Due to the similarity between the centralized safety-LEMPC and safety-LMPC formulations as mentioned in Remark 4.4, an iterative distributed design for the safety-LMPC formulation, with the implementation strategy and associated closed-loop stability and feasibility proofs, would follow that of this section, with $t_s = t_0$.*

Remark 4.7 *An assumption throughout this chapter is that the time to calculate the solutions to the distributed safety-LEMPC problems is much less than the sampling time such that the calculations can be considered instantaneous. When such short time scales are assumed for the computations, an alternative to terminating the iterations as soon as the condition on $V(\tilde{x}^{tot}(t))$ is not met would be to re-perform optimization iteration c with different initial guesses to try to meet the condition on $V(\tilde{x}^{tot}(t))$ at the iteration and potentially improve the optimality of the implemented solutions from a safety and economics perspective.*

4.4 Application to a chemical process example

In this section, we demonstrate the advantages of the proposed Safety-DLEMPC schemes over the centralized Safety-LEMPC of Eq. 4.7 by applying them to a benchmark catalytic reactor example. The closed-loop economic performance and the on-line computation time needed to solve the three Safety-LEMPC optimization problems are the key performance metrics. A chemical process example (catalytic reactor) is considered in which the oxidation of ethylene to ethylene oxide takes place in a non-isothermal continuous stirred tank reactor (CSTR) according to the following

reactions:

$$C_2H_4 + \frac{1}{2}O_2 \xrightarrow{r_1} C_2H_4O \tag{R1}$$

$$C_2H_4 + 3O_2 \xrightarrow{r_2} 2CO_2 + 2H_2O \tag{R2}$$

$$C_2H_4O + \frac{5}{2}O_2 \xrightarrow{r_3} 2CO_2 + 2H_2O \tag{R3}$$

Table 4.1: Values of the dimensionless parameters of the ethylene oxidation CSTR.

$A_1 = 92.8$	$B_2 = 10.39$	$\gamma_2 = -7.12$
$A_2 = 12.66$	$B_3 = 2170.57$	$\gamma_3 = -11.07$
$A_3 = 2412.71$	$B_4 = 7.02$	
$B_1 = 7.32$	$\gamma_1 = -8.13$	

To remove the heat generated by the exothermic reactions, a cooling jacket is used. The dimensionless material and energy balances for the catalytic reactor are developed in[77] where the rate laws for the reactions use the nonlinear Arrhenius reaction in.[12] The dimensionless mass and energy balances for this process are described by the following equations:[77]

$$\frac{dx_1(t)}{dt} = u_1(1 - x_1x_4) \tag{4.24a}$$

$$\frac{dx_2(t)}{dt} = u_1(u_2 - x_2x_4) - A_1e^{\frac{\gamma_1}{x_4}}(x_2x_4)^{0.5} - A_2e^{\frac{\gamma_2}{x_4}}(x_2x_4)^{0.25} \tag{4.24b}$$

$$\frac{dx_3(t)}{dt} = -u_1x_3x_4 + A_1e^{\frac{\gamma_1}{x_4}}(x_2x_4)^{0.5} - A_3e^{\frac{\gamma_3}{x_4}}(x_3x_4)^{0.5} \tag{4.24c}$$

$$\frac{dx_4(t)}{dt} = \frac{u_1}{x_1}(1 - x_4) + \frac{B_1}{x_1}e^{\frac{\gamma_1}{x_4}}(x_2x_4)^{0.5} + \frac{B_2}{x_1}e^{\frac{\gamma_2}{x_4}}(x_2x_4)^{0.25} + \frac{B_3}{x_1}e^{\frac{\gamma_3}{x_4}}(x_3x_4)^{0.5} - \frac{B_4}{x_1}(x_4 - u_3) \tag{4.24d}$$

The resulting dimensionless dynamic model of this reactor has four states x_1, x_2, x_3, and x_4 and three manipulated inputs u_1, u_2, and u_3. The four dimensionless states represent the reactor gas mixture density, ethylene concentration, ethylene oxide concentration, and temperature

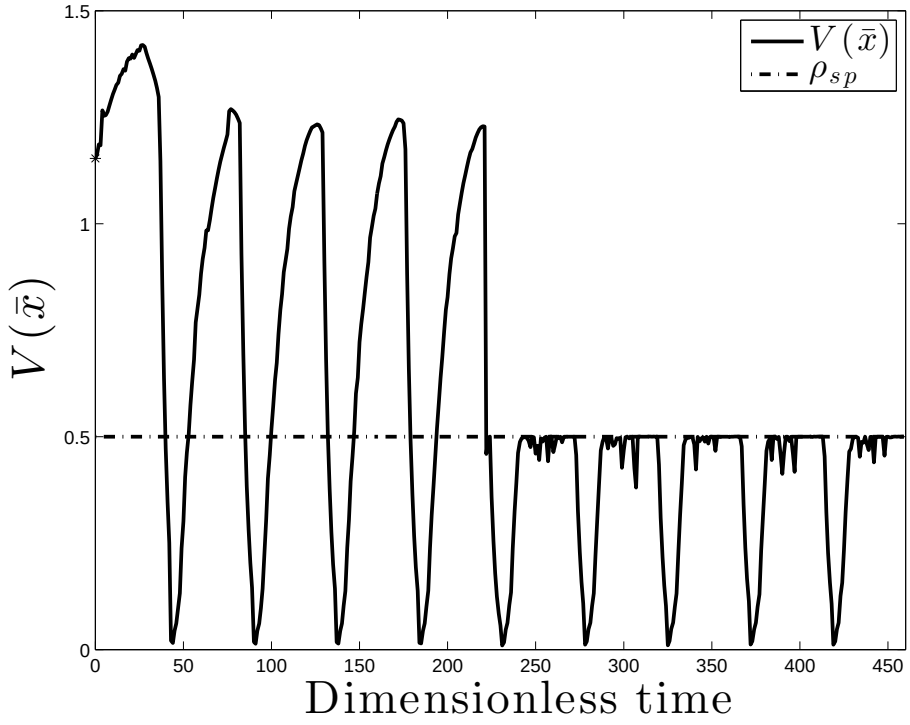

Figure 4.3: Evolution of the Lyapunov function value of the closed-loop state under the centralized Safety-LEMPC

in the reactor, respectively. The three dimensionless inputs u_1, u_2, and u_3 of the reactor are the feed volumetric flow rate, the concentration of ethylene in the feed, and the coolant temperature, respectively. The values of the parameters of this model are presented in Table 4.1. Due to the physical constraints on the control actuators, the manipulated inputs are bounded (i.e., $u_1 \in [0.0704,\ 0.7042]$, $u_2 \in [0.2465,\ 2.4648]$, $u_3 \in [0.6,\ 1.1]$). The economic performance index of the catalytic reactor is the average yield of ethylene oxide where the yield is defined by:

$$Y(t_f) = \frac{\int_{t_0}^{t_f} u_1(\tau)x_3(\tau)x_4(\tau)\, d\tau}{\int_{t_0}^{t_f} u_1(\tau)u_2(\tau)\, d\tau} \tag{4.25}$$

where t_f is the operating period. A limitation on the amount of reactant material that may be fed

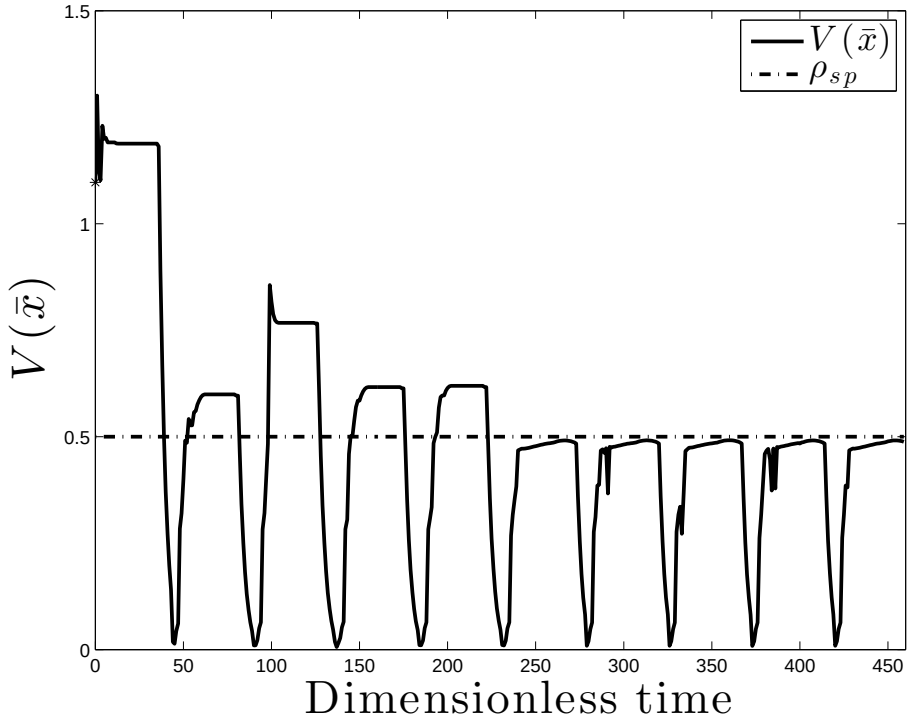

Figure 4.4: Evolution of the Lyapunov function value of the closed-loop state under the Safety-S-DLEMPC

to the reactor is fixed by the following integral material constraint:

$$\frac{1}{t_f}\int_{t_0}^{t_f} u_1(\tau)u_2(\tau)\, d\tau = 0.175. \tag{4.26}$$

Since the denominator of Eq. 4.25 is fixed over the length of operation, the various Safety-LEMPC schemes considered in this chapter will maximize the following stage cost:

$$L_e(x,u) = u_1 x_3 x_4. \tag{4.27}$$

The dynamic model of the catalytic reactor has an open-loop asymptotically stable steady-state that satisfies the integral material constraint of Eq. 4.26 with $x_s^T = [x_{1s}\ x_{2s}\ x_{3s}\ x_{4s}] =$ $[0.998\ \ 0.424\ \ 0.032\ \ 1.002]$ which corresponds to the steady-state input $u_s^T = [0.35\ \ 0.5\ \ 1.0]$. The contractive constraint of Eqs. 4.7h, 4.8j, and 4.21j was not imposed in all the simulations be-

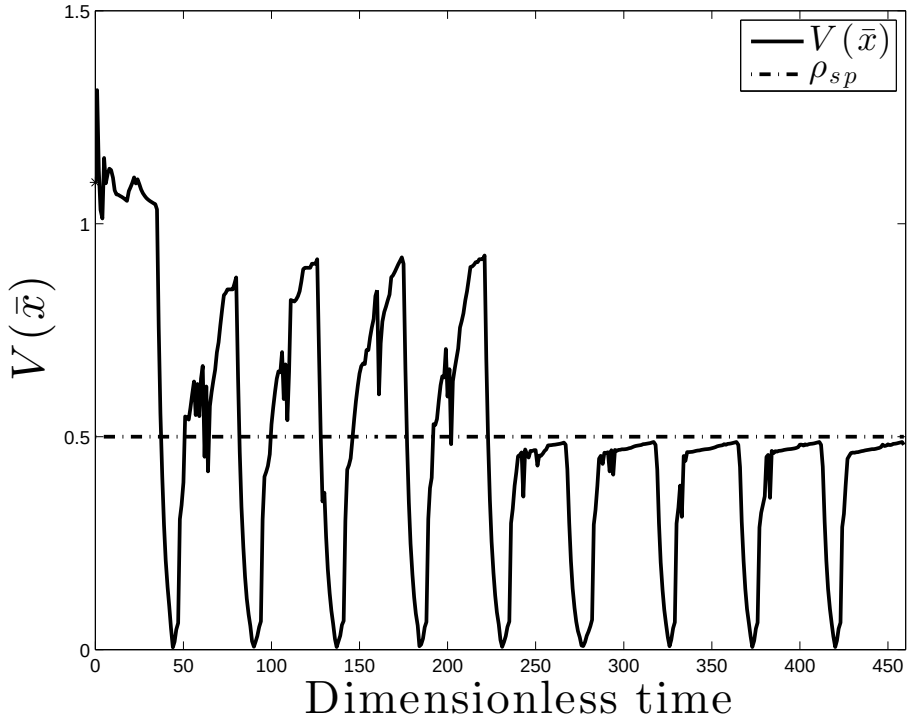

Figure 4.5: Evolution of the Lyapunov function value of the closed-loop state under the Safety-I-DLEMPC

low since closed-loop stability under the various Safety-LEMPC schemes is not an issue for the region of operation considered for the dynamic model of this reactor. In order to determine the safety level set, a characterization of the closed-loop stability region Ω_ρ of the dynamic model of the reactor is required. To estimate the stability region Ω_ρ, a PI controller $h^T(x) = [h_1(x)\ h_2(x)\ h_3(x)]$ is implemented in a sample-and-hold fashion for the three manipulated inputs (i.e., $h_a(x) = K_{P_a}(x_a - x_{as}) + \frac{1}{\tau_a}\int_0^t (x_a - x_{as})dt,\ a = 1,2,3$, where $K_{P_1} = 3.0,\ K_{P_2} = 0.105,\ K_{P_3} = 0.1,\ \tau_1 = 0.00001,\ \tau_2 = 0.0002081$, and $\tau_3 = 0.005$). The centralized and distributed Safety-LEMPC schemes are implemented with a shrinking prediction horizon that covers the entire operating window $t_p = 47$; specifically, at the beginning of the l^{th} operating window, the prediction horizon was set to t_p/Δ and the horizon was decreased by one at each sampling period where $\Delta = 1$. At the beginning of the $(l+1)^{th}$ operating window where $l = 0,\ldots,9$, the prediction horizon is reinitialized to t_p/Δ. To satisfy the material constraint of Eq. 4.26, this constraint is im-

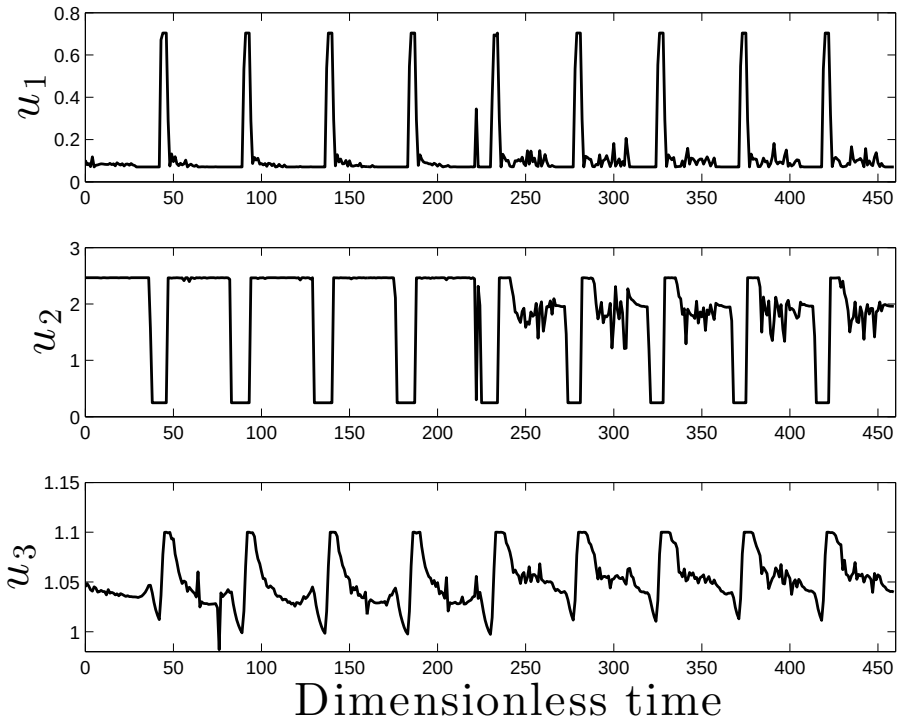

Figure 4.6: Input trajectories computed by the centralized Safety-LEMPC

posed over the ten operating windows (i.e., the average molar flow rate of ethylene must be equal to 0.175 at the end of each operating interval of length t_p). The dynamic model of the catalytic reactor is simulated numerically by using the explicit Euler method with a step size of 10^{-5}, while the step size used for the model within the Safety-LEMPC optimization problems is 0.0005. All the optimization problems were solved using the interior-point solver Ipopt.[90]

We use a quadratic Lyapunov function of the form $V(\bar{x}) = \bar{x}^T P \bar{x}$ to estimate the stability region of the closed-loop system under $h(x)$ where $P = \text{diag}([1\ \ 1\ \ 1\ \ 1])$. The notation $\bar{x}$ denotes the process state vector in deviation form (i.e., $\bar{x} = x - x_s$). The safety level set $\Omega_{\rho_{sp}}$ is chosen to operate the closed-loop process in a relatively small region around the steady-state to avoid the boundary of the stability region. Following this technique and using the Lyapunov function $V(\bar{x})$, the values of ρ and ρ_{sp} were chosen to be 2.1 and 0.5, respectively. As a result of the integral material constraint of Eq. 4.26, the inputs u_1 and u_2 are optimized by one Safety-DLEMPC (i.e., $\bar{u}_1^T = [u_1\ u_2]$), as well as K_c, while only u_3 is computed by another (i.e., $\bar{u}_3 = u_3$ with $K_c \equiv 0$) for

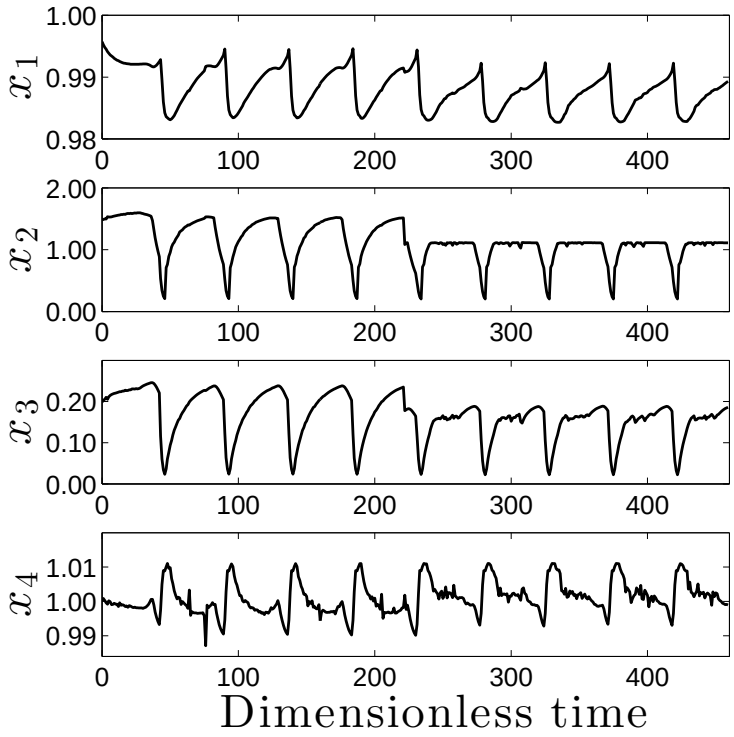

Figure 4.7: Process state trajectories under the centralized Safety-LEMPC

both iterative and distributed Safety-DLEMPC's.

The termination condition for the Safety-I-DLEMPC algorithm was to stop iterating the optimization problem when the cost function at the current iteration is less than or equal to the cost function at the previous iteration. In this example, the condition on the value of $V(\tilde{x}^{tot})$ along the closed-loop state trajectories of the nominal system under the control actions calculated by the two iterative distributed controllers was not checked between iterations, but no issues with feasibility occurred during the iterations performed. Ipopt was forced to stop optimizing the problem after 100 iterations to take real-time computation considerations into account.

Table 4.2: The average yield and computation time under the safety-LEMPC strategies.

Strategy	Yield (%)	Computation Time (s)
Safety-S-DLEMPC	9.85	6.64
Safety-I-DLEMPC	9.94	5.59
Centralized Safety-LEMPC	10.15	16.87

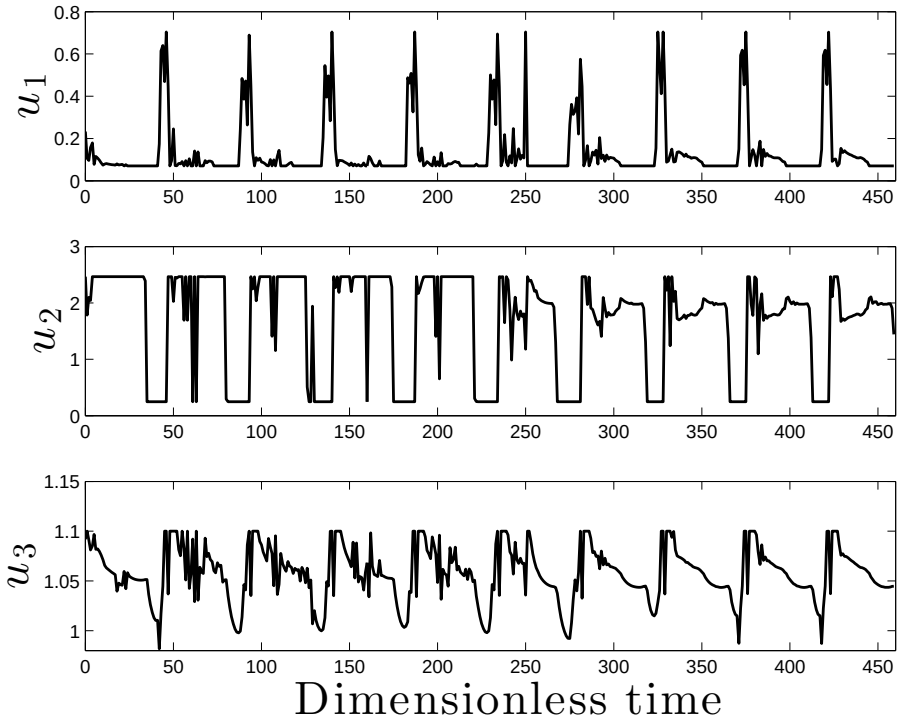

Figure 4.8: Input trajectories computed by the Safety-I-DLEMPC

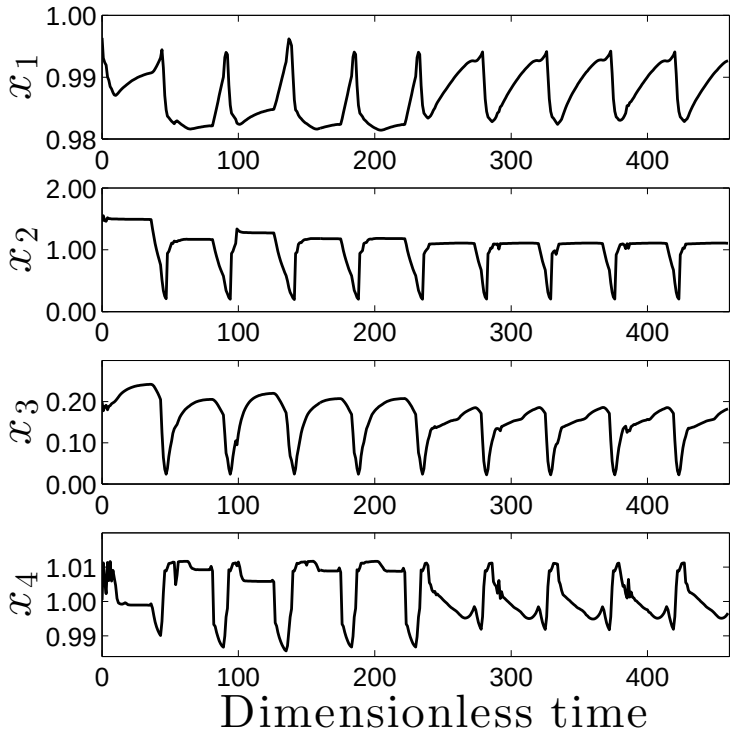

Figure 4.9: Process state trajectories under the Safety-S-DLEMPC

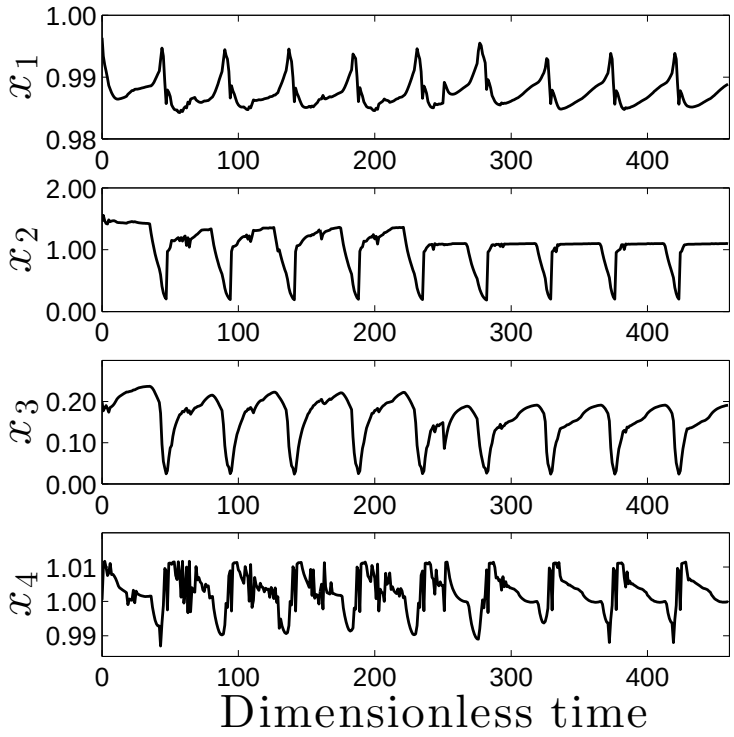

Figure 4.10: Process state trajectories under the Safety-I-DLEMPC

The computation time for the Safety-S-DLEMPC is evaluated as the sum of the computation times of Safety-S-DLEMPC 1 and Safety-S-DLEMPC 2 at each sampling time because the distributed controllers are evaluated in sequence which means that the minimal time to obtain a solution is the sum of the evaluated times of all controllers. However, the computation time for one iteration of the Safety-I-DLEMPC is computed as the maximum computation time of the two optimization problems because the distributed controllers are evaluated in parallel which implies that the minimal time to obtain a solution is the largest computation time among all the Safety-I-DLEMPC controllers.

In these simulations, the catalytic reactor was initiated far from $\Omega_{\rho_{sp}}$ with $x^T(t_0) = [0.9818 \;\; 1.4566 \;\; 0.1987 \;\; 1.0523]$ (i.e., $V(x(t_0)) = 1.09 > \rho_{sp} = 0.5$). Starting at $t_k = 222$, the safety logic unit requests the closed-loop state to move toward the safety level set under the centralized and distributed Safety-LEMPC schemes. Figures 4.3, 4.5 and 4.4 show the Lyapunov function value of the closed-loop states under the centralized Safety-LEMPC and iterative and sequential

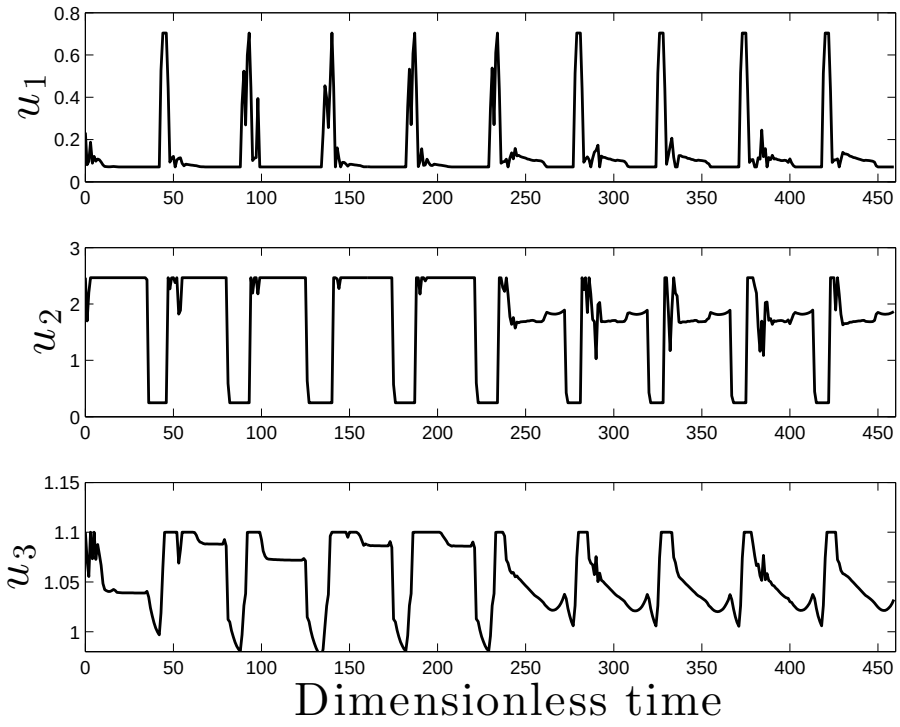

Figure 4.11: Input trajectories computed by the Safety-S-DLEMPC

Safety-DLEMPC controllers, respectively. From these figures, the closed-loop states under the three controllers successfully entered the safety level set after one sampling time (i.e., $V(t_k) < \rho_{sp}$ where $t_k = 223$). Figures 4.7, 4.6, 4.10, 4.8, 4.9 and 4.11 represent the closed-loop state trajectories and the manipulated input trajectories of the centralized Safety-LEMPC and iterative and sequential Safety-DLEMPC controllers, respectively. As in,[17] the centralized Safety-LEMPC, the Safety-S-DLEMPC, and the Safety-I-DLEMPC dictate periodic operation (i.e., the ethylene is distributed in a non-uniform fashion with respect to time) to maximize the yield of ethylene oxide. The input trajectories u_1 and u_2 satisfied the material constraint of Eq. 4.26 under all Safety-LEMPC schemes. Figure 4.7, Figure 4.10 and Figure 4.9 show that the closed-loop trajectories under all the Safety-LEMPC schemes changed after the safety-based constraints are activated at $t_k = 222$ while periodic operation is still maintained. Due to the nonlinearity and non-convexity of the optimization problem, the Safety-I-DLEMPC under the termination condition described above terminates most of the time after the second iteration so that the $c = 1$ solution is applied (i.e.,

the cost function at the first iteration is generally greater than or equal to the cost function at the second iteration). Table 4.2 shows the average yield and average computation time required to solve each of the three optimization problems over the ten operating windows. From Table 4.2, the average yield of ethylene oxide under the centralized safety-LEMPC and distributed (iterative and sequential) safety-LEMPC's is similar. The centralized safety-LEMPC of Eq. 4.7 requires over 150% more computation time than both the iterative and the sequential safety-DLEMPC's. Additionally, the average yield of ethylene oxide over ten operating periods under the PI controllers is 5.34%; the average yield under the centralized safety-LEMPC is 90% better than that under the PI controllers.

Remark 4.8 *Even though the dynamic model of the reactor of Eq. 4.24 does not explicitly follow the class of systems of Eq. 4.1 due to the bilinear term in the right hand side of the second differential equation (i.e., $u_1(u_2 - x_2x_4)$), the system can be reformulated to take a form in the class of systems of Eq. 4.1. Since the manipulated input u_2 only appears in that term and the safety DLEMPC 1 solves for the inputs u_1 and u_2 together in one optimization problem due to the material constraint of Eq. 4.26, a new variable $u_4 = u_1u_2$ can be introduced to make the process model appear in the form of the class of systems of Eq. 4.1 (input affine with inputs u_1, u_3 and u_4). Furthermore, as is demonstrated above, the distributed control methodology of this chapter performed well for this example.*

4.5 Conclusion

In this chapter, sequential and iterative Safety-DLEMPC schemes were proposed as alternatives to centralized Safety-LEMPC that may have less on-line computation time while achieving similar closed-loop performance and safety constraints satisfaction. An implementation strategy and mathematical formulation for the Safety-Sequential-DLEMPC design and the Safety-Iterative-DLEMPC design were developed. The main objective of the two distributed Safety-LEMPC schemes is to improve the computation time with respect to the centralized Safety-LEMPC while

maintaining similar closed-loop performance. For a sufficiently small sampling period, proofs of recursive feasibility and closed-loop stability of a class of nonlinear systems under the Safety-S-DLEMPC and Safety-I-DLEMPC formulations in the presence of uncertainty were given. Using a catalytic reactor example, the proposed iterative and sequential Safety-DLEMPC strategies were able to yield comparable closed-loop performance while significantly decreasing the on-line computation time compared to that required to solve the centralized Safety-LEMPC. This illustrates that distributed implementation may allow Safety-LEMPC to be implemented on processes where the computation time of the centralized implementation strategy exceeds the controller sampling time.

Chapter 5

Process Operational Safety Using Model Predictive Control Based on A Process Safeness Index

5.1 Introduction

The development of a systematic methodology for coordinating safety and control systems poses fundamental challenges; for example, metrics must be developed that can be shared by the control and safety systems to indicate safe or unsafe system operation, and constraints need to be developed for MPC that prevent the closed-loop state from entering unsafe regions based on the developed safety metrics while maintaining closed-loop stability and feasibility. A metric that can unify control and safety systems considerations could improve the designs of both of these systems. Motivated by the above considerations, in this chapter a metric termed the Safeness Index that is a function of the closed-loop process state is developed. The Safeness Index indicates the relative safeness of the process state in state-space based on past process data, first-principles models and traditional safety analysis tools. The safety system as well as the control system can then incorporate this index by setting thresholds on the value of this index upon which the actions of the

control and safety systems are based. An LEMPC design and implementation strategy that uses the Safeness Index as a hard constraint and maintains closed-loop stability is rigorously developed to demonstrate the incorporation of this metric within a process control system. The proposed Safeness Index framework can be applied to both existing systems and new process systems and technologies. Using a chemical process example, the proposed LEMPC is compared with that of an LEMPC scheme that does not incorporate the Safeness Index-based constraint in terms of its ability to maintain the process state within a region where the value of the Safeness Index is less than a desired threshold. The results of this chapter originally appeared in.[26]

5.2 Preliminaries

5.2.1 Notation

The operator $|\cdot|$ signifies the 2-norm of a vector. The transpose of a vector x is represented by the symbol x^T. The symbol Ω_ρ is used to denote a level set of a sufficiently smooth, positive definite scalar-valued function $V(x)$ and is defined by $\Omega_\rho := \{x \in R^n : V(x) \leq \rho\}$. The operator '/' denotes set subtraction, that is, $A/B := \{x \in R^n : x \in A, x \notin B\}$. The symbol $S(\Delta)$ denotes the family of piecewise constant, right-continuous functions with a fixed time interval $\Delta \geq 0$. The initial time instant is denoted by t_0. A function $\alpha(\cdot) : [0, a) \to [0, \infty)$ belongs to class $\mathcal{K}$ if it is strictly increasing and continuous, and $\alpha(0) = 0$.

5.2.2 Class of Nonlinear Process Systems

The class of nonlinear process systems considered in this chapter is that of the general form:

$$\dot{x} = f(x, u, w) \tag{5.1}$$

where $x \in \mathbb{R}^n$, $u \in U \subset \mathbb{R}^m$, and $w \in \mathbb{R}^l$ are the state, input, and disturbance vectors, respectively. We assume that f is a locally Lipschitz vector function of its arguments and that the state of the

system of Eq. 5.1 is synchronously sampled at time instances $t_k = t_0 + k\Delta,\ k = 0, 1, \ldots$, where Δ is the sampling period and t_0 is the initial time. The disturbance $w(t)$ is bounded within the set $W := \{w \in \mathbb{R}^l : |w| \leq \theta, \theta > 0\}$ (i.e., $w(t) \in W$). We assume that the origin is an equilibrium point of the unforced nominal system which implies that $f(0,0,0) = 0$.

5.2.3 Nonlinear System Stabilizability Assumption

We consider systems of the form of Eq. 5.1 for which Assumption 5.1 holds.

Assumption 5.1 *There exists a locally Lipschitz feedback control law $h(x) \in U$ with $h(0) = 0$ for the nominal closed-loop system of Eq. 5.1 (i.e., $w(t) \equiv 0$) that renders the origin of the closed-loop system with $u = h(x)$ asymptotically stable for all $x \in D \subseteq R^n$ where D is an open neighborhood of the origin, when applied continuously in the sense that there exists[49,63] a continuously differentiable Lyapunov function $V(x)$ for the nominal closed-loop system and class $\mathcal{K}$ functions $\alpha_i(\cdot)$, $i = 1,2,3,4$ such that the following inequalities hold:*

$$\begin{aligned} \alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|) \\ \frac{\partial V(x)}{\partial x} f(x, h(x), 0) \leq -\alpha_3(|x|) \\ \left| \frac{\partial V(x)}{\partial x} \right| \leq \alpha_4(|x|) \\ h(x) \in U, \quad \forall\, x \in D \subseteq R^n \end{aligned} \tag{5.2}$$

The stability region of the closed-loop system under the feedback control law that meets Assumption 5.1 is defined as a level set of the Lyapunov function within D where Eq. 5.2 holds, and it is denoted by Ω_ρ. Techniques for designing explicit stabilizing control laws for different classes of nonlinear systems can be found in works such as.[27,35,53,59]

When x is maintained within the stability region Ω_ρ, we have from the continuity of x, the local Lipschitz property of f, and the continuous differentiability of $V(x)$ that there exist positive

constants M, L_x, L_w, $L_x^{'}$ and $L_w^{'}$ such that the following inequalities hold:

$$|f(x(t),u(t),w(t))| \leq M \tag{5.3}$$

$$|f(x,u,w) - f(x^*,u,0)| \leq L_x|x-x^*| + L_w|w| \tag{5.4}$$

$$\left|\frac{\partial V(x)}{\partial x} f(x,u,w) - \frac{\partial V(x^*)}{\partial x} f(x^*,u,0)\right| \leq L_x'|x-x^*| + L_w'|w| \tag{5.5}$$

for all $x, x^* \in \Omega_\rho$, $u_i \in U_i$, $i = 1,\ldots,m$, and $w \in W$.

When $h(x)$ is applied to the nonlinear process in a sample-and-hold fashion, the following proposition holds.

Proposition 5.1 *(c.f.[43,72]) Let Assumption 5.1 hold, V be the Lyapunov function that satisfies Eq. 5.2, and Ω_ρ be the resulting stability region. Then if $\rho_s < \rho$, θ, and Δ satisfy*

$$-\alpha_3(\alpha_2^{-1}(\rho_s)) + L_x'M\Delta + L_w'\theta \leq -\varepsilon_w/\Delta \tag{5.6}$$

for $\varepsilon_w > 0$, then for any $x(t_0) \in \Omega_\rho$,

$$V(x(t)) \leq V(x(t_k)),\ \forall\, t \in [t_k, t_{k+1}) \tag{5.7}$$

and

$$V(x(t_{k+1})) < V(x(t_k)) \tag{5.8}$$

along the closed-loop state trajectory of the sampled-data system

$$\dot{x}(t) = f(x(t),h(x(t_k)),w(t)),\ \forall\, t \in [t_k, t_{k+1}),\ k = 0,1,\ldots \tag{5.9}$$

when $x(t_k) \in \Omega_\rho / \Omega_{\rho_s}$. If $\rho_{\min} < \rho$ where

$$\rho_{\min} = \max\{V(x(t+\Delta)) : V(x(t)) \leq \rho_s\} \tag{5.10}$$

then the closed-loop state is always bounded in Ω_ρ and is (uniformly) ultimately bounded in $\Omega_{\rho_{\min}}$ as follows:

$$\limsup_{t\to\infty} x(t) \in \Omega_{\rho_{\min}} \,. \tag{5.11}$$

$\rho_{\min}$ in the above proposition is defined as the maximum value of the Lyapunov function that will be reached under any sample-and-hold control action (not necessarily $h(x(t_k))$) that meets the input constraints in the presence of bounded disturbances by the end of a sampling time when $x(t_k) \in \Omega_{\rho_s}$.

5.2.4 Lyapunov-based EMPC

The control design that will be investigated in this chapter will be a specific type of EMPC termed Lyapunov-based economic model predictive control (LEMPC). LEMPC is a dual-mode optimization-based control strategy that utilizes the Lyapunov-based controller $h(x)$ to define two modes of operation where closed-loop stability is guaranteed in the presence of uncertainty.[43] The mathematical formulation of LEMPC is as follows:

$$\min_{u\in S(\Delta)} \quad \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau))\, d\tau \tag{5.12a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{5.12b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{5.12c}$$

$$u(t) \in U,\ \forall\, t \in [t_k, t_{k+N}) \tag{5.12d}$$

$$V(\tilde{x}(t)) \leq \rho_e,\ \forall\, t \in [t_k, t_{k+N})$$

$$\text{if } x(t_k) \in \Omega_{\rho_e} \tag{5.12e}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0)$$

$$\text{if } x(t_k) \notin \Omega_{\rho_e} \tag{5.12f}$$

where the decision variable of the LEMPC of Eq. 5.12 is the piecewise constant input trajectory $u(t)$ defined over the prediction horizon $N\Delta$ (i.e., $u \in S(\Delta)$). The optimization problem of Eq. 5.12 optimizes the economic measure $L_e(x(t),u(t))$ (Eq. 5.12a) which defines the cost function, subject to a nominal process model (Eq. 5.12b). The initial condition of the nominal process model of Eq. 5.12b comes from a measurement of the process state at the current sampling time t_k (Eq. 5.12c). Eq. 5.12d shows that the calculated control actions $u(t)$ are restricted to the set U over the prediction horizon.

Under the first operation mode (Eq. 5.12e), the LEMPC optimizes the economic measure $L_e(x(t),u(t))$ in a time-varying fashion while maintaining the predicted closed-loop state within the set Ω_{ρ_e} which is a subset of the stability region Ω_ρ. The region Ω_{ρ_e} is defined such that if the measured process state at a sampling time t_k is within Ω_{ρ_e}, then at the next sampling time t_{k+1}, it is still within Ω_ρ, even in the presence of bounded disturbances. Under the second operation mode, the LEMPC utilizes a contractive constraint (Eq. 5.12f) to ensure that the control action for the first sampling period of the prediction horizon for the closed-loop system forces the state along a path that causes the Lyapunov function value to decrease between two sampling periods. The two-mode operating strategy of LEMPC ensures that the stability region Ω_ρ is a forward invariant set.[43] The LEMPC produces a set of N input vectors $u^*(t|t_k)$, $t \in [t_k, t_{k+N})$, after solving at each sampling time, but only the input vector $u^*(t_k|t_k)$ corresponding to the first sampling period of the prediction horizon is applied to the process in a sample-and-hold fashion.

Remark 5.1 *The explicit stabilizing controller $h(x)$ provides a feasible control action for both modes of operation of Eq. 5.12 for $x(t_k) \in \Omega_\rho$. In other words, if the measured state is within Ω_{ρ_e}, then applying $h(\tilde{x}(t_j))$, $\forall\ t \in [t_j, t_{j+1})$, $j = k, \ldots, k+N-1$, throughout each corresponding sampling period in the prediction horizon guarantees that the predicted state will be maintained within Ω_{ρ_e} over the prediction horizon (i.e., Eq. 5.12e is met by $h(x)$ implemented in sample-and-hold throughout the prediction horizon). If the measured state leaves Ω_{ρ_e}, then applying the explicit stabilizing controller $h(x(t_k))$ for the first sampling period of the prediction horizon, with any other sample-and-hold control action that meets the input constraint of Eq. 5.12d throughout*

the rest of the prediction horizon ($h(\tilde{x}(t_j)), \forall\, t \in [t_j, t_{j+1}),\ j = k+1, \ldots, k+N-1$, is a control law that satisfies this requirement by Eq. 5.2) is a feasible solution to the LEMPC of Eq. 5.12 since it meets the contractive constraint of Eq. 5.12f applied at the first sampling period of the prediction horizon.[43]

5.3 Safeness Index-Based Control and Safety System Design

In this section, we develop the concept of a process Safeness Index for use in the control and safety systems. We then discuss techniques that can allow the safety system, as well as the control system, to incorporate this index by setting thresholds on the value of this index that cause the control and safety systems to take certain actions. Finally, we develop a controller that utilizes this index (specifically, the LEMPC scheme of Eq. 5.12 with a hard constraint related to a threshold on the Safeness Index, termed Safeness Index-based LEMPC) with an implementation strategy that is proven to maintain closed-loop stability of a nonlinear process.

5.3.1 Development of a Process Safeness Index

To effectively integrate the process control and safety systems, it is desirable to develop a Safeness Index that is a function of the process (closed-loop) state only and indicates the safeness of a plant as a whole, given multivariable interactions and interactions between units, which cannot be evaluated with the typical component-by-component safety analyses that are usually performed. Such a state-based index is consistent with the sentiments of various researchers who have stated that a process does not become unsafe automatically, but takes a gradual trajectory in that direction (e.g.,[58]). The index also benefits from being a function only of the current state; much of the safety thinking in the process industries is a cause-and-effect-type relationship for which the reasons that a state became unsafe are important to the fact that it is unsafe. By developing a Safeness Index that is a function of the current state only, engineers do not need to think of every possible failure mechanism of a system and whether the system is on any of those many paths to understand

whether a system is unsafe, but need only characterize where it is on the safeness spectrum based on its present condition. Another benefit of a state-based index is that it can capture safety information even for unmeasured states if an appropriate state estimator is developed, which is not a capability of traditional safety system designs based on process measurements only.

Though the development of a Safeness Index has great promise for improving process safety, the form of the Safeness Index will be process-dependent, and thus a methodology for determining the value of the Safeness Index must be developed. A possible methodology would be to define a function $S(x)$ (the Safeness Index) that can take one of two values at each state-space location (e.g., 0 for 100% safe operating states and 1 for less safe states). An important consideration in the development of a Safeness Index, however, is its intended use in developing constraints in optimization-based control and triggers for the alarm, emergency shut-down, and relief systems, and the binary form of $S(x)$ discussed above would be ineffective for enhancing the safety systems (e.g., the binary function cannot indicate whether the system is near an unsafe state but has not yet reached it, which would be required to trigger elements of the safety system based on $S(x)$ exceeding a threshold). To address these issues, this section develops a systematic methodology for formulating a (not necessarily binary) Safeness Index for a given process based on two factors: 1) $S(x)$ is a function of the process (closed-loop) state only (the path followed to arrive at the state is immaterial; this enables a departure from the limiting cause-and-effect mentality traditionally utilized in chemical process safety system design and accident analysis,[57] and furthermore, allows the safeness of the system given the controller's effects and limitations to be analyzed); and 2) $S(x)$ indicates the safeness of a plant as a whole, given multivariable interactions and interactions between units, which cannot be evaluated with the component-by-component safety analyses that are usually performed.

The proposed methodology requires analysis, for a given process, of information on past accidents, the results of industrial safety studies, first-principles models, and past operating data to determine both the states that should explicitly appear in $S(x)$ and also a suitable functional dependence of $S(x)$ on these states, as shown in Figure 5.1. The first step in this procedure is to

determine which states to incorporate in $S(x)$. Initially, an extensive literature review of accidents and their causes (e.g.,[32, 50, 52, 87]) can be performed to determine guidelines for states that should be considered based on which states (e.g., temperature, pressure) took abnormal values when past accidents occurred. This study can be used to analyze what kinds of accidents might occur at the plant under consideration, which may have also been investigated for the plant through standard industrial safety analysis techniques (e.g., what-if analyses and HAZOP studies). Any states that are tied to the abnormal situations expected both from the literature review and the safety analyses should be selected for inclusion in $S(x)$. A first-principles model may also reveal that other states should be considered that were perhaps neglected in the qualitative analyses in the early steps due to complexities in the system that are revealed through analyzing the dynamics. For example, it should be checked that $S(x)$: 1) Incorporates states from the model that are known to lead to unsafe/explosive conditions based on the chemistry of the reactions involved (e.g., reactions associated with ignition at certain temperatures[30]) or the reactor material limitations (e.g., high temperature or high pressure can lead to reactor rupture); 2) Incorporates states that have a large influence on other states in the reactor that affect process safety; 3) Incorporates all states that influence the safeness of the process, even if these states are unmeasurable or only affect the safeness of the process when they take values far from their values under normal process operating conditions (states that do not indicate the safeness of the process under any condition would not need to be included, however). Analyses like these may be aided through closed-loop simulations of the process from various initial conditions in state-space. Process operating data may also aid in determining which states to incorporate in $S(x)$. For example, process data corresponding to time periods of normal, near-miss (e.g., situations in which the safety system is triggered[78]), and accident operating conditions may be analyzed to determine which states reach values at the near-miss and accident conditions that are significantly different from their values under normal operation, and then include such states in $S(x)$.

After the states to be included in $S(x)$ are identified, it is necessary to determine the functional form of $S(x)$. This functional form should be developed to facilitate the purpose of defining $S(x)$,

which is to set thresholds on its value that can be used to distinguish between safe and unsafe operating regions in state-space to cause the control and safety systems to take specific actions based on the threshold values. This indicates that two primary principles should guide the choice of the functional form of $S(x)$: 1) It should be designed so that $S(x)$ will have a significantly larger value when the closed-loop state reaches an unsafe operating region than when it is in a safe operating region; 2) It should incorporate controller limitations and therefore increase rapidly as the boundary of the stability region in which closed-loop stability is guaranteed is approached to reflect that beyond this boundary, the process cannot be guaranteed to be controllable, which is considered an unsafe scenario. Principle 1 may require careful design of $S(x)$ due to potential differences in magnitude of the various states of the process. For example, consider a case in which temperature and concentration of corrosive reactant play a role in the safeness of a chemical process. In many cases, the order of magnitude of the temperature will be greater than that of the concentration, with the result that without careful design of $S(x)$, the reactant concentration may take unsafe values for values of $S(x)$ that are not significantly greater than its value under normal operating conditions or even may be the same as the value of $S(x)$ under normal operating conditions if the temperature drops when the concentration increases. Such a design of $S(x)$ would not facilitate meaningful thresholds being set on its value for use in the control and safety systems; this indicates that scaling of process states or giving $S(x)$ a nonlinear dependence on certain process states may be required when developing the functional form of the Safeness Index. Other cases in which scaling or nonlinearities in $S(x)$ may be beneficial include cases when a process state results in an unsafe condition only when it takes an extreme value, or when the process dynamics are such that there are values of the state vector from which, according to the process dynamics, the state quickly can move from those values to states that pose safety concerns (e.g., if there is a certain pressure P_1 within a reactor from which, under certain conditions, the reactor pressure can quickly elevate to a level that would rupture the reactor, $S(x)$ should become large as this pressure P_1 is reached).

Stability of the closed-loop state can dictate the functional form of the Safeness Index, which

allows safety systems that are triggered by a threshold on $S(x)$ to incorporate considerations from the control system in identifying unsafe operating regions. An example of a characterizable form of $S(x)$ that increases as the boundary of the stability region is approached (and, for convenience, is scaled by ρ so that it lies between 0 and 1 and takes a value of 1 on the boundary of the stability region) is a quadratic form (e.g., $S(x) = x^T x/\rho$). A Safeness Index with a functional form that gives states further from an open-loop unstable operating steady-state a higher value of $S(x)$ may be beneficial if the open-loop trajectories initiated near this steady-state evolve toward an open-loop stable steady-state with a temperature above the allowable operating limits (even when the open-loop unstable steady-state is stabilized by a controller and $S(x)$ is evaluated for the closed-loop state, actuator outputs are typically limited such that beyond a certain region in state-space, the available control energy may no longer prevent the state from reaching unsafe conditions).

5.3.2 Choosing Thresholds for $S(x)$ for Use within the Control and Safety Systems

After the functional form of $S(x)$ is determined, it is necessary to set thresholds on $S(x)$ that can be used to modify the control design and trigger the safety system. Figure 5.1 illustrates the approach for developing the thresholds on $S(x)$ to be used in the control and safety systems. The control, alarm, emergency shut-down, and relief systems should utilize different thresholds on $S(x)$ for consistency with their independence and also for consistency with standard industrial practice in which the alarms are only activated when the control system does not maintain the process state within a region where all variables instrumented with alarms are within their recommended ranges, and the emergency shut-down system is only activated after another set of thresholds on the instrumented variables is exceeded.[62] However, because the control system is the first line of defense against unsafe situations (i.e., the safety systems would ideally not be activated frequently for a well-controlled process), the threshold S_{TH} on $S(x)$ utilized by an optimization-based control design should be lower than the thresholds utilized in the safety systems. If the controller then computes control actions subject to a constraint that it should maintain the closed-loop state pre-

dictions in a region where the Safeness Index value is less than S_{TH}, false alarms (i.e., activations of the safety system in regions of state-space where the controller guarantees closed-loop stability and guarantees that it can drive the state back into a region where $S(x) < S_{TH}$) may be avoided. Motivated by this, methods for determining S_{TH} will be the focus of this section.

To set the value of S_{TH}, past accidents, the results of industrial safety studies, and first-principles models can be analyzed to gain insight into which values of the states may become large during unsafe conditions and what their expected magnitudes may be to aid in setting S_{TH}. In addition, process data can be valuable for setting S_{TH}. Specifically, past operating data can be labeled as corresponding to safe or unsafe process operating conditions by: 1) labeling the data as "safe" if no alarms were triggered during the time period corresponding to that data set; 2) labeling the data as "safe" if very few (e.g., one or two) alarms sounded during the time period corresponding to the data set, but the closed-loop state subsequently re-entered an operating region where no alarms were triggered without intervention from the operator, emergency shut-down, or relief systems; and 3) labeling data as "unsafe" if a number of alarms sounded during the time period corresponding to that data set. Subsequently, the value of $S(x)$ can be evaluated for each of the labeled data sets. The threshold S_{TH} can then be chosen as a value that is below the minimum value of $S(x)$ observed in the "unsafe" data sets that is significantly different from the values of $S(x)$ observed during "safe" operation to allow "safe" and "unsafe" operating conditions to be appropriately distinguished in the control design. S_{TH} should be somewhat conservatively chosen to allow for other thresholds to be used in triggering the safety system (i.e., the process should not exhibit any negative consequences immediately after $S(x) > S_{TH}$, because that gives the safety system no opportunity to prevent accidents). However, the conservatism in the control design should not be extreme to the point that operating in the region where $S(x) < S_{TH}$ impacts process economics unnecessarily.

Another important consideration in setting S_{TH} for use in an optimization-based control design that utilized stability constraints based on Ω_ρ (e.g., LEMPC) is to ensure that there exist states in the stability region for which $S(x) < S_{TH}$ (if not, there would be no safe operating condition in the

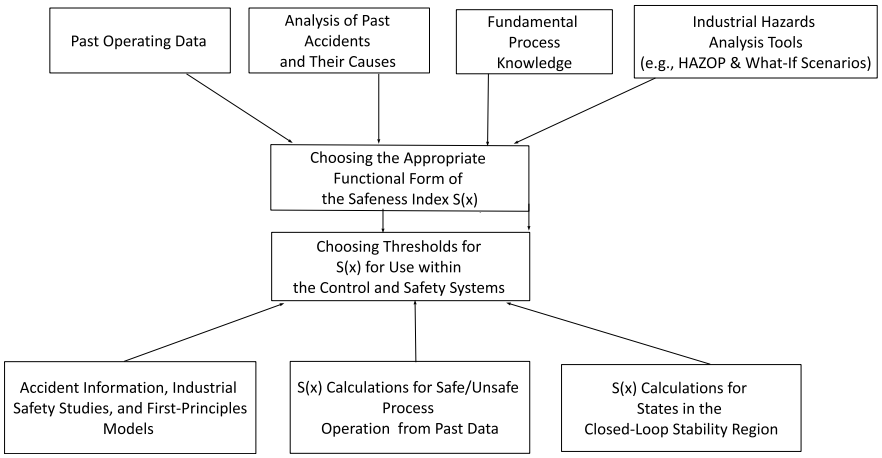

Figure 5.1: Systematic methodology to construct $S(x)$ and its thresholds.

region in which the controller ensures closed-loop stability). Therefore, off-line calculations for the value of the Safeness Index $S(x)$ within the stability region Ω_ρ could be performed to validate that with the chosen form of $S(x)$ and the chosen value of S_{TH}, this condition is satisfied. Also, S_{TH} should be set such that when the process is operated in the region where $S(x) < S_{TH}$, none of the thresholds on individual measured variables traditionally utilized to trigger the alarm, emergency shut-down, or relief systems is surpassed to prevent frequent and unnecessary activation of the safety systems at a plant. The concept of a set of states in state-space being partitioned into "safe" and "unsafe" regions utilizing a threshold on the Safeness Index is illustrated in Figure 5.2, where the boundary between the regions occurs at a threshold value $S(x) = S_{TH}$. An illustration of how to define $S(x)$ and S_{TH} will be performed in the context of a chemical process example in Section 5.4.

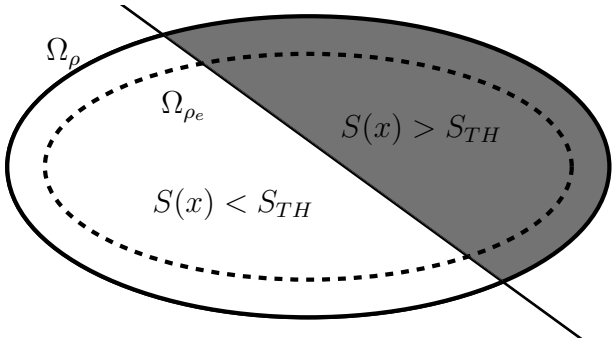

Figure 5.2: Example of level set partitioned into "safe" ($S(x) < S_{TH}$), and "unsafe" ($S(x) > S_{TH}$) regions.

Remark 5.2 *The triggering mechanism of the alarm and emergency shut-down systems, and elements of the relief system that can be automated, can be augmented to include not only the traditional triggers based on individual measured variables exceeding or falling below their recommended ranges, but also triggers based on the value of the Safeness Index exceeding threshold values. This can help prevent missed alarms because it allows the safety system to account for multivariable interactions and unmeasured states that may be important in assessing process safety but have traditionally been unavailable to these systems. The thresholds on $S(x)$ utilized by the safety system can come from analyzing industrial safety studies, past accidents, first-principles models, and process operating data as in the evaluation of S_{TH}, except that the thresholds should be tiered so that the thresholds utilized in the alarm, emergency shut-down, and relief systems reflect increasing levels of concern over the process operating conditions. While the control system designs will only use S_{TH} to bound $S(x)$, the various levels of the safety system should be activated by tiered thresholds for consistency with industrial practice. In addition, the threshold value set for the control system should be chosen such that the value of the Safeness Index $S(x)$ of the process state during the short excursions from the safety region (i.e., $S(x) \leq S_{TH}$) does not reach the threshold value of the alarm system. In other words, the threshold value S_{TH} utilized by the control system should be chosen such that "short excursions" of the process state do not violate the threshold value of the safety system to avoid triggering safety alarms.*

Remark 5.3 *$S(x)$ can be defined to take any values within the set of real numbers, but because we consider that the states and inputs are bounded, $S(x)$ will only practically take values within the control system within a subset of the real numbers that correspond to points in state-space where closed-loop stability is guaranteed (i.e., Ω_ρ).*

5.3.3 Safeness Index-Based LEMPC Formulation

In the remainder of this chapter, we analyze an optimization-based control design (specifically, an LEMPC) that incorporates a hard constraint requiring that the controller compute control actions that maintain the predicted process state within the region where $S(x) < S_{TH}$. This control design

may improve process economic performance and be less conservative than the safety-based control design developed in Chapter 2, where safety-based constraints were included within LEMPC that were triggered when a measurement of the closed-loop state was outside a safe Lyapunov level set of operation termed the safety region $\Omega_{\rho_{sp}} \subset \Omega_{\rho}$. The level set-based method of triggering safety-based constraints is conceptually the same as developing a binary Safeness Index function that evaluates to either its value corresponding to safe operation within $\Omega_{\rho_{sp}}$ (indicating that the process is within a 100% safe operating region and that the safety-based constraints do not need to be activated) or its value corresponding to unsafe operation outside of $\Omega_{\rho_{sp}}$ (indicating that the process is not operating in a safe region and that the safety-based constraints should be activated). Whenever the process state is within a safe region of operation and the safety-based constraints are not applied, the process economics are optimized while the process state is maintained within this safe region of operation. Thus, process safety is ensured while the process profit is maximized. Despite the guaranteed closed-loop stability and recursive feasibility properties of this method,[6] as well as its economic optimization capabilities, it may be unnecessarily restrictive for many processes. For example, regions within which $S(x)$ is below a desired threshold may not be level sets of a Lyapunov function, and trying to find the largest Lyapunov level set within a region where $S(x)$ is less than the threshold may cause the level set to be quite small, which can greatly reduce the economic optimality of process operation within this small region compared to allowing the process to operate within the entire region where $S(x)$ is less than a desired threshold. Furthermore, the threshold value on $S(x)$ may not be a hard threshold (i.e., it may reflect that the process should not in general operate above the threshold, but that short excursions into the region where $S(x)$ is greater than a desired threshold are acceptable; this may be the case, for example, for a reforming tube of a steam methane reformer, for which minor excursions of temperature above the design temperature may reduce the tube lifetime, e.g., increasing the temperature by 20 K can half the lifetime,[55] but will not result in immediate negative consequences). Therefore, allowing $S(x)$ above a threshold value for finite periods of time may be perfectly acceptable from a process safety perspective, and may also be economically beneficial by allowing the closed-loop state to move

throughout a larger region of state-space during process operation.

To allow for this less restrictive process operating strategy (for processes for which leaving the region where $S(x)$ is less than a threshold value for finite periods of time is acceptable) while still utilizing LEMPC to allow for economic optimality of process operation, the threshold on the Safeness Index can be used as a hard constraint within LEMPC to form a Safeness Index-based LEMPC design. Specifically, we propose the following formulation of the Safeness Index-based LEMPC:

$$\max_{u(t)\in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau))\, d\tau \tag{5.13a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{5.13b}$$

$$u(t) \in U,\ \forall\, t \in [t_k, t_{k+N}) \tag{5.13c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{5.13d}$$

$$V(\tilde{x}(t)) \leq \rho_e,\ \forall\, t \in [t_k, t_{k+N}) \quad \text{if } x(t_k) \in \Omega_{\rho_e} \tag{5.13e}$$

$$S(\tilde{x}(t)) \leq S_{TH},\ \forall\, t \in [t_k, t_{k+N}) \quad \text{if } S(x(t_k)) \leq S_{TH} \tag{5.13f}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0), \quad \text{if } x(t_k) \in \Omega_\rho / \Omega_{\rho_e} \text{ or } t_k > t_s \text{ or } S(x(t_k)) > S_{TH} \tag{5.13g}$$

where the notation follows that in Eq. 5.12. The time t_s is a pre-determined time after which it is desired to apply the constraint of Eq. 5.13g at each sampling time. The constraint of Eq. 5.13e defines the first operation mode of the LEMPC of Eq. 5.12 and allows the cost function of Eq. 5.13a to be maximized while keeping the predicted closed-loop state within Ω_{ρ_e}. When the contractive constraint of Eq. 5.13g is not concurrently applied (as it would be if $x(t_k) \in \Omega_{\rho_e}$ but either $t_k > t_s$ or $S(x(t_k)) > S_{TH}$), the constraints of Eqs. 5.13e-5.13f allow the controller to enforce

a potentially dynamic operating policy to maximize the process economics while maintaining the predicted closed-loop state within the region where $S(\tilde{x}(t)) \leq S_{TH}$ (Eq. 5.13f), defined as the safety zone (i.e., the region where the Safeness Index is less than the threshold value for $S(x)$). The hard constraint on the Safeness Index (Eq. 5.13f) may also be enforced concurrently with the contractive constraint if the measured state is within the safety zone but either $x(t_k) \in \Omega_\rho / \Omega_{\rho_e}$ or $t_k > t_s$. The role of the contractive constraint is to maintain boundedness of the closed-loop state within the stability region Ω_ρ, and also to drive the closed-loop state back into the safety zone in finite time when it leaves this region when the LEMPC is feasible at every sampling time (an implementation strategy utilizing the LEMPC of Eq. 5.13 in combination with a Lyapunov-based controller implemented in sample-and-hold is proposed below that is guaranteed to provide closed-loop stability of a nonlinear process within Ω_ρ and to drive the closed-loop state back into the safety zone whenever it exits this region even if the LEMPC is not feasible at every sampling time). Unlike the stability region Ω_ρ, the safety zone is not necessary a forward invariant set because as stated above, the threshold S_{TH} set on the Safeness Index may define a region that is irregularly shaped; for instance, Figure 5.2 shows one possible safety zone that is not necessarily a forward invariant set and is irregularly shaped. An important point regarding this formulation is that the origin of the nominal closed-loop system of Eq. 5.1 is always assumed to be inside the safety zone (i.e., $S(x) \leq S_{TH}$ when $x = 0$).

The fact that the safety zone is not necessarily a forward invariant set means that feasibility of the LEMPC of Eq. 5.13 cannot be guaranteed whenever the constraint of Eq. 5.13f is activated (i.e., whenever $S(x(t_k)) \leq S_{TH}$). This means that though the explicit stabilizing controller $h(\tilde{x}(t_j))$, $\forall\ t \in [t_j, t_{j+1}),\ j = k, \ldots, k+N-1$, is guaranteed to meet the constraints of Eqs. 5.13b-5.13e and the constraint of Eq. 5.13g since these constraints form the LEMPC formulation of Eq. 5.12 (Remark 5.1) and will thus be a feasible control action whenever $S(x(t_k)) > S_{TH}$, this control law is no longer guaranteed to be feasible when $S(x(t_k)) \leq S_{TH}$. In other words, it is possible that the only feasible control action that satisfies Eqs. 5.13b-5.13d and Eqs. 5.13e and/or 5.13g (depending on whether the conditions that activate Eqs. 5.13e and 5.13g are active) is $h(x(t_k))$ in

the first sampling period with either $h(\tilde{x}(t_j)), \forall\, t \in [t_j, t_{j+1}),\ j = k+1,\ldots,k+N-1$ (if Eq. 5.13e is active) or any other control actions that meet Eq. 5.13c if Eq. 5.13e is not active but Eq. 5.13g is (Remark 5.1). However, controlling a system under $h(x(t_k)), \forall\, t \in [t_k, t_{k+1})$ (and $h(\tilde{x}(t_j)), \forall\, t \in [t_k, t_{k+1}),\ j = k+1,\ldots,k+N-1$) only guarantees that the Lyapunov function of the closed-loop state will decrease between two sampling periods, though it may cause the Lyapunov function to decrease along a path that causes the closed-loop state to leave the safety zone while it decreases the Lyapunov function value. If $h(x(t_k)), \forall\, t \in [t_k, t_{k+1})$ (and $h(\tilde{x}(t_j)), \forall\, t \in [t_j, t_{j+1}),\ j = k+1,\ldots,k+N-1$) is the only feasible solution to the constraints of Eqs. 5.13b-5.13d and Eqs. 5.13e and/or 5.13g, but it drives the closed-loop state out of the safety zone, the optimization problem of Eq. 5.13 becomes infeasible. To deal with this infeasibility issue, we introduce the following implementation strategy for the Safeness Index-based LEMPC that utilizes the solution of the Safeness Index-based LEMPC whenever it is feasible and applies the Lyapunov-based controller in sample-and-hold instead when the LEMPC is infeasible (closed-loop stability of a nonlinear process under this implementation strategy is proven in the next section):

1. At t_k, a measurement of the current state $x(t_k)$ is received from the sensors; go to Step 2.
2. Solve the Safeness Index-based LEMPC problem of Eq. 5.13 and then go to Step 3.
3. If the Safeness Index-based LEMPC problem of Eq. 5.13 is feasible, then go to Step 3a. Else, go to Step 3b.
   (a) Apply $u^*(t_k|t_k)$ from the Safeness Index-based LEMPC solution to the nonlinear process in a sample-and-hold fashion, and then go to Step 4.
   (b) Apply the explicit stabilizing controller $h(x)$ in a sample-and-hold fashion (i.e., $u(t) = h(x(t_k)); \forall\, t \in [t_k, t_{k+1})$). Then go to Step 4.
4. Go to Step 1 ($k \leftarrow k+1$).

Remark 5.4 *It was noted that the Safeness Index-based LEMPC is appropriate for processes for which finite-time excursions of the closed-loop state outside of the safety zone are acceptable from*

a process safety standpoint (as will be shown in the next section, these excursions of $S(x)$ above S_{TH} do not jeopardize the closed-loop stability of the process because the closed-loop state is always maintained within Ω_ρ under this implementation strategy) and for which there are substantial economic benefits for allowing such excursions. However, for nonlinear processes that cannot tolerate leaving the safety zone, the Safeness Index-based LEMPC can be formulated to handle such processes. In these cases, $S(x)$ can be defined as the Lyapunov function scaled by the value of the Lyapunov function at the boundary of the stability region (i.e., $S(x) = x^T Px/\rho$), and S_{TH} for use within Eq. 5.13f can be chosen sufficiently lower than the value of the Lyapunov function corresponding to the actual desired threshold to guarantee closed-loop stability and feasibility within the safety zone even in the presence of disturbances/plant-model mismatch. In this case, the safety zone will be a forward invariant set and closed-loop stability of a nonlinear process initiated within Ω_ρ, guaranteed entry to the safety zone and maintenance of the state within the safety zone after it enters this region, and recursive feasibility of the resulting Safeness Index-based LEMPC would follow from[6,43] if the region where $V(x) \leq S_{TH}$ includes a neighborhood of the origin into which the Lyapunov-based controller implemented in sample-and-hold would drive the closed-loop state. In this case, $h(\tilde{x}(t_j)), \forall\, t \in [t_j, t_{j+1}),\ j = k, \ldots, k+N-1$, would be a feasible solution to the Safeness Index-based LEMPC when the process is initialized within the safety zone.

Remark 5.5 *The fact that $S(x)$is developed based on the closed-loop state is vital to its effective use within the safety system. Another type of constraint that may be examined as a Safeness Index-based constraint in the context of MPC is a constraint that allows the closed-loop state to increase above a threshold value of $S(x)$ but only for a limited time. This may be the case, for example, for a reforming tube of a steam methane reformer, for which increasing the temperature slightly above the design temperature may decrease tube lifetime but would not be expected to immediately rupture the tube if it had not been in service for long. For this case, the constraint of Eq. 5.13fcan be replaced with $t_{sum} \leq t_A$ to enforce that the total time t_{sum} in an operating period during which $S(x) > S_{TH}$ be no more than a time length t_A.*

Remark 5.6 *In both the Safeness Index-based LEMPC formulation of Eq. 5.13 and the modifica-*

tion that Remark 5.5 introduces to the LEMPC formulation of Eq. 5.13, the value of the Safeness Index for the predicted state trajectory ($S(\tilde{x})$) is constrained to be no greater than the threshold S_{TH} over the prediction horizon $N\Delta$ or to not exceed S_{TH} for more than t_A. However, in some chemical processes the safety of the process is a matter of cumulative behavior of the process state over time; for example, if the temperature of a reactor is above a certain value over some time, that may diminish the material strength of the reactor. In such scenarios, the integration (summation) of the value of $S(x)$ over a given period of time will indicate the safeness of the process. To account for this safety property, the Safeness Index constraint of Eq. 5.13f can be replaced with

$$\int_0^t S(x(t'))dt' \leq S_b \tag{5.14}$$

where S_b is a parameter dependent on the material strength of the process equipment.

Remark 5.7 *In this chapter, we have focused on the case that a single upper bound S_{TH} is defined on $S(x)$ for use in the control system, though the methodology for the development of thresholds on $S(x)$ and the constraints on $S(x)$ in the control design can be extended to the case that there are both an upper bound and a lower bound on $S(x)$ that indicate the safety of the process (and similarly in the safety system).*

Remark 5.8 *The discussion in this section shows that another consideration for setting S_{TH} is the control system design that will incorporate this threshold. Because $S(x)$ may exceed S_{TH} under the Safeness Index-based LEMPC design (though the state will always be driven back into the safety zone), the threshold S_{TH} may be more conservatively chosen when such a control design is used. If, as in Remark 5.4, $S(x)$ is a Lyapunov function, the region in which it is desired to maintain the closed-loop state for safety reasons may be more directly tied to the values of the process states as the state approaches unsafe conditions because the controller can guarantee that the state will not leave the region where $S(x)$ is below a desired value. Also, to guarantee closed-loop stability under the implementation strategy of the control design presented in this section (which will be shown in the next section), the safety zone has to be defined to include $\Omega_{\rho_{\min}}$, which affects both*

the form of $S(x)$ and its thresholds.

5.3.4 Feasibility and Stability Analysis

In this subsection, we present sufficient conditions to show that the state of the closed-loop system of Eq. 5.1 under the Safeness Index-based LEMPC implementation strategy is guaranteed to enter the safety zone where $S(x) \leq S_{TH}$ in finite time and to remain within the stability region Ω_ρ at all times. Moreover, we prove that the closed-loop state is guaranteed to be ultimately bounded in a small region containing the origin. To proceed, we first re-state two propositions from[43] to define functions and parameters needed for the proof of closed-loop stability of a nonlinear process the Safeness Index-based LEMPC implementation strategy, and then present Theorem 1 that gives sufficient conditions for the proof of closed-loop stability of a nonlinear process under the Safeness Index-based LEMPC implementation strategy.

Proposition 5.2 (c.f.[43,67]) *Consider the systems*

$$\begin{aligned} \dot{x}_a(t) &= f(x_a(t), u(t), w(t)) \\ \dot{x}_b(t) &= f(x_b(t), u(t), 0) \end{aligned} \tag{5.15}$$

with initial states $x_a(t_0) = x_b(t_0) \in \Omega_\rho$. There exists a $\mathscr{K}$ function $f_W(\cdot)$ such that

$$|x_a(t) - x_b(t)| \leq f_W(t - t_0), \tag{5.16}$$

for all $x_a(t), x_b(t) \in \Omega_\rho$ and all $w(t) \in W$ with

$$f_W(\tau) = \frac{L_w \theta}{L_x}(e^{L_x \tau} - 1). \tag{5.17}$$

Proposition 5.3 (c.f.[43,67]) *Consider the Lyapunov function $V(\cdot)$ of the system of Eq. 5.1. There*

exists a quadratic function $f_V(\cdot)$ *such that*

$$V(x) \leq V(\hat{x}) + f_V(|x-\hat{x}|) \tag{5.18}$$

for all $x, \hat{x} \in \Omega_\rho$ *with*

$$f_V(s) = \alpha_4(\alpha_1^{-1}(\rho))s + M_v s^2 \tag{5.19}$$

where M_v *is a positive constant.*

Theorem 5.1 *Consider the system of Eq. 5.1 in closed-loop under the implementation strategy (Steps 1-4) of the Safeness Index-based LEMPC of Eq. 5.13 based on a controller* $h(x)$ *that satisfies the conditions of Eq. 5.2. Let* $\varepsilon_w > 0$, $\Delta > 0$, $\rho > \rho_e > \rho_s > 0$ *satisfy*

$$\rho_e \leq \rho - f_V(f_W(\Delta)) \tag{5.20}$$

and

$$-\alpha_3(\alpha_2^{-1}(\rho_s)) + L_x' M\Delta + L_w'\theta \leq -\varepsilon_w/\Delta. \tag{5.21}$$

If $x(t_0) \in \Omega_\rho$, $\rho_{\min} \leq \rho$ *and* $N \geq 1$ *where* $\rho_{\min}$ *is defined as in Eq. 5.10 and where the compact set* $\Omega_{\rho_{\min}}$ *satisfies*

$$\Omega_{\rho_{\min}} \subseteq \{x \in \Omega_\rho \ : \ S(x) \leq S_{TH}\}, \tag{5.22}$$

then the closed-loop state $x(t)$ *of Eq. 5.1 is guaranteed to enter the safety zone in finite time when* $x(t_0) \in \Omega_\rho$, *to be bounded within* Ω_ρ *at all times, and to be ultimately bounded in* $\Omega_{\rho_{\min}}$.

Proof 5.1 *The proof consists of two parts. The first part is the proof that an input trajectory with characterizable properties exists for a nonlinear process operated under Steps 1-4 of the Safeness Index-based LEMPC implementation strategy when* $x(t_0) \in \Omega_\rho$. *The second part is the proof of the three results of Theorem 5.1 given these characterizable properties.*

Part 1: To prove the results of Theorem 5.1, it is necessary to prove that the inputs applied to the process from the Safeness Index-based LEMPC implementation strategy are characterizable so that closed-loop stability of a nonlinear process under such input trajectories can be investigated. According to the implementation strategy, in a given sampling period, one of two cases will occur: 1) the Safeness Index-based LEMPC of Eq. 5.13 is a feasible optimization problem and $u(t_k|t_k)$ is applied to the process for $t \in [t_k, t_{k+1})$; 2) the Safeness Index-based LEMPC of Eq. 5.13 is not a feasible optimization problem and $h(x(t_k))$ is applied for $t \in [t_k, t_{k+1})$. In the first case when the Safeness Index-based LEMPC is feasible, this means that a feasible solution was determined that satisfied the constraints of Eqs. 5.13b-5.13g for the nominal closed-loop system for the given sampling period. In the second case when the LEMPC is not feasible and $h(x)$ is applied in a sample-and-hold fashion, the conditions of Proposition 5.1 hold for the given sampling period. Thus, for any given sampling period, the conditions met by the control actions that are implemented can be characterized, and therefore the conditions met by the input trajectory applied throughout time can be characterized and thus used in analyzing closed-loop stability.

Part 2: We now prove the results of Theorem 5.1. Specifically, we prove that if the closed-loop state of the nonlinear process under the Safeness Index-based LEMPC implementation strategy is initialized within the stability region Ω_ρ, even outside the safety zone (i.e., $S(x(t_0)) > S_{TH}$), then within finite time the closed-loop state will enter the safety zone. Furthermore, we prove that for any $x(t_0) \in \Omega_\rho$, the closed-loop state remains within the stability region Ω_ρ at all times. We also show that if $t_k > t_s$, then the closed-loop state will be ultimately bounded in a compact set containing the origin.

To prove that the closed-loop state will always enter the safety zone in finite time under the Safeness Index-based LEMPC implementation strategy when it is either initiated outside of this region or leaves this region while operated in closed-loop when the process is initiated from any initial condition $x(t_0) \in \Omega_\rho$, we first show that the closed-loop state under either a feasible solution to the Safeness Index-based LEMPC of Eq. 5.13 or under $h(x)$ implemented in sample-and-hold will drive the closed-loop state toward the set $\Omega_{\rho_{\min}}$ throughout a given sampling period, where

$\Omega_{\rho_{\min}}$ *is within the safety zone from Eq. 5.22. When* $S(x(t_k)) > S_{TH}$ *and the Safeness Index-based LEMPC is feasible at* t_k*, the contractive constraint of Eq. 5.13g is active. In,*[43] *it is proven that when the conditions of Eqs. 5.20-5.21 are satisfied,* $V(x(t)) \leq V(x(t_k)),\ \forall\ t \in [t_k, t_{k+1})$*, and* $V(x(t_{k+1})) < V(x(t_k))$ *along the trajectories of the closed-loop system under an LEMPC containing the contractive constraint, even in the presence of bounded disturbances, when* $x(t_k) \notin \Omega_{\rho_s} \subseteq \Omega_{\rho_{\min}}$*. If the Safeness Index-based LEMPC is infeasible at* t_k*,* $h(x(t_k))$ *is applied, which causes Eqs. 5.7-5.8 to hold when* $x(t_k) \notin \Omega_{\rho_s} \subseteq \Omega_{\rho_{\min}}$*. This means that in a given sampling period, whether* $u^*(t_k|t_k)$ *is applied or* $h(x(t_k))$ *according to the implementation strategy, the Lyapunov function value of the closed-loop state is guaranteed to decrease throughout the sampling period. At each sampling time until* $S(x(t_k)) \leq S_{TH}$*, the contractive constraint of Eq. 5.13g will remain active and therefore the Lyapunov function value will continue to decrease. Therefore, the closed-loop state will either enter the safety zone in finite time (before it enters* $\Omega_{\rho_{\min}}$*), or Eq. 5.13g will continue to be applied within the LEMPC and the Safeness Index-based LEMPC implementation strategy will continue to cause* $V(x(t)) \leq V(x(t_k)),\ \forall\ t \in [t_k, t_{k+1})$*, until the closed-loop state enters* $\Omega_{\rho_{\min}}$*. Because Eq. 5.22 holds, and the closed-loop state enters* $\Omega_{\rho_{\min}}$ *in finite time from any initial condition in* Ω_ρ*, the closed-loop state is thus guaranteed to enter the safety zone, regardless of its shape, within finite time, from any* $x(t_k) \in \Omega_\rho$ *where* $S(x(t_k)) > S_{TH}$*, even in the presence of disturbances.*

To prove that Ω_ρ *is a forward invariant set under the Safeness Index-based LEMPC implementation strategy (i.e., when* $x(t_0) \in \Omega_\rho$*,* $x(t) \in \Omega_\rho\ \forall\ t \in [t_0, \infty)$*), we first demonstrate that in a given sampling period, if* $x(t_k) \in \Omega_\rho$*, then* $x(t) \in \Omega_\rho \forall t \in [t_k, t_{k+1})$ *both in the case that the Safeness Index-based LEMPC of Eq. 5.13 has a feasible solution throughout the prediction horizon* $N\Delta$*, and in the case that it does not and* $h(x(t_k))$ *is applied for* $t \in [t_k, t_{k+1})$*. When the Safeness Index-based LEMPC is feasible, the stability results of*[43] *hold because they are based only on feasibility of the Lyapunov-based stability constraints of Eqs. 5.13e and 5.13g and do not depend on whether other constraints such as Eq. 5.13f are enforced. Specifically, if* $x(t_k) \in \Omega_{\rho_e}$ *such that the constraint of Eq. 5.13e is active, then* $\tilde{x}(t_{k+1}) \in \Omega_{\rho_e}$ *and* $x(t) \in \Omega_\rho \forall t \in [t_k, t_{k+1})$ *from the constraint of Eq. 5.13e, Propositions 5.2-5.3, and Eq. 5.20. If* $x(t_k) \in \Omega_\rho / \Omega_{\rho_e}$*, then Eq. 5.13g is active, which decreases the*

Lyapunov function value between two sampling periods and thus ensures that the closed-loop state enters a lower level set (and thus cannot exit Ω_ρ). When the Safeness Index-based LEMPC has no feasible solution throughout the prediction horizon, then $h(x(t_k))$ will be applied between two sampling times, which will decrease the Lyapunov function between the two sampling times and thus ensure that the closed-loop state does not leave Ω_ρ in that sampling period. If $x(t_0) \in \Omega_\rho$, then recursive application of the property that $x(t_k) \in \Omega_\rho$ ensures that $x(t) \in \Omega_\rho \forall t \in [t_k, t_{k+1})$, starting with $k = 0$, shows that the Safeness Index-based LEMPC implementation strategy maintains the closed-loop state within Ω_ρ at all times.

To prove that if $t_k > t_s$, the closed-loop state under the Safeness Index-based LEMPC implementation strategy is ultimately bounded in $\Omega_{\rho_{\min}}$, we note that under this condition, the contractive constraint of Eq. 5.13g will be active within the LEMPC, and either the LEMPC will be feasible or $h(x(t_k))$ will be applied to the process throughout the sampling period. As noted above, control actions generated from either the LEMPC or from $h(x(t_k))$ under this condition will continue to decrease the Lyapunov function value until the closed-loop state enters the compact set $\Omega_{\rho_{\min}}$ in a finite time. From the definition of $\Omega_{\rho_{\min}}$, once the closed-loop state enters $\Omega_{\rho_{\min}}$, if $u^*(t_k|t_k)$ that meets the contractive constraint or $h(x(t_k))$ is then applied to the process, decreasing the Lyapunov function value until the closed-loop state enters Ω_{ρ_s}, the closed-loop state cannot leave $\Omega_{\rho_{\min}}$. The proof of this is analogous to the proof of ultimate boundedness in.[43]

Remark 5.9 *It is noted that if Eq. 5.22 holds, then if $t_k > t_s$ and the closed-loop state has entered $\Omega_{\rho_{\min}}$ and is ultimately bounded there, the closed-loop state is within the safety zone for all subsequent times. This shows that if it is found that the closed-loop state under the Safeness Index-based LEMPC implementation strategy is spending an undesirable length of time above the safety threshold, the current sampling time t_k can be set to t_s to cause the Safeness Index-based LEMPC implementation strategy to drive the closed-loop state into a region where the threshold on the Safeness Index is always met and to maintain closed-loop operation in this region until the value of S_{TH} can be redesigned so that the Safeness Index-based LEMPC causes the closed-loop state to remain below a desired threshold for more of the operating time.*

5.4 Application to a Chemical Process Example

In this section, a chemical process example is provided to illustrate the ability of the Safeness Index-based LEMPC to maintain the closed-loop state within a region where $S(x(t_k)) \leq S_{TH}$ when the LEMPC of Eq. 5.12 would not compute an input trajectory that achieves this. The chemical process example is a well-mixed, non-isothermal continuous stirred tank reactor (CSTR) where an irreversible second-order exothermic reaction takes place. The reaction transforms a reactant A to a product B ($A \rightarrow B$). The feedstock of the CSTR consists of pure A and the inlet concentration of A is C_{A0}. The inlet temperature and feed volumetric flow rate of the reactor are T_0 and F, respectively. The CSTR is equipped with a heating jacket that heats/cools the reactor at a heat rate Q. The process has two states, C_A for the concentration of the reactant species A and T for the reactor temperature, and these states are taken to evolve according to the mass and energy balances derived from first-principles modeling of the CSTR with standard chemical engineering assumptions as follows:

$$\frac{dC_A}{dt} = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{R_g T}} C_A^2 \tag{5.23a}$$

$$\frac{dT}{dt} = \frac{F}{V}(T_0 - T) + \frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{R_g T}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{5.23b}$$

The notation ΔH, k_0, E, and R_g represent the enthalpy of reaction, pre-exponential constant, activation energy, and ideal gas constant, respectively. The reactor volume V, heat capacity C_p, and fluid density ρ_L within the reactor are assumed constant (process parameter values are listed in Table 5.1). The dynamic model of Eq. 5.23 is integrated numerically by using the explicit Euler method with an integration time step of $h_c = 10^{-5}\ hr$.

The manipulated inputs are the concentration C_{A0} of the reactant species A in the feed and the heat input/removal rate Q. The process of Eq. 5.23 has multiple steady-states with associated steady-state input values $[C_{A0s}\ Q_s] = [4\ \frac{kmol}{m^3}\ 0\ \frac{kJ}{hr}]$. The CSTR is operated around an open-loop asymptotically stable steady-state that occurs at $[C_{As}\ T_s] = [1.2\ \frac{kmol}{m^3}\ 438\ K]$. The dynamic model

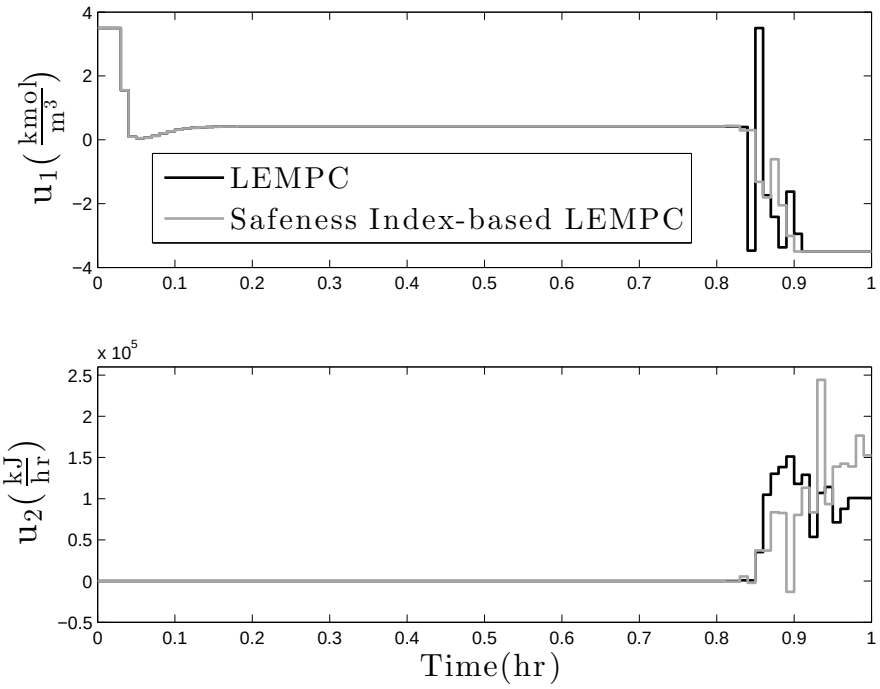

Figure 5.3: Manipulated input profiles for the closed-loop CSTR under the LEMPC design of Eq. 5.12 and under the Safeness Index-based LEMPC design of Eq. 5.13 for the initial condition $x_{int}^T = [0\ \frac{kmol}{m^3}\ 0\ K]$.

of Eq. 5.23 is in the following class of nonlinear systems:

$$\dot{x}(t) = \tilde{f}(x(t)) + g_1(x(t))u_1(t) + g_2(x(t))u_2(t) \tag{5.24}$$

where $x(t)$ and $u(t)$ denote the state and the manipulated inputs of the CSTR in deviation variable form (i.e., $x^T = [C_A - C_{As}\ T - T_s]$ is the state vector and $u^T = [C_{A0} - C_{A0s}\ Q - Q_s]$ is the manipulated input vector), $\tilde{f}^T = [\tilde{f}_1\ \tilde{f}_2]$ is a vector containing the terms in the CSTR model that do not include u_1 or u_2, and $g_i^T = [g_{i1}\ g_{i2}]$ $(i = 1,2)$ is a vector containing the terms in the CSTR model that multiply u_1 (for $i = 1$) or u_2 (for $i = 2$). The magnitudes of the manipulated inputs are bounded as follows: $|u_1| \leq 3.5\ \frac{kmol}{m^3}$ and $|u_2| \leq 5 \times 10^5\ \frac{kJ}{hr}$. The control objective is to maximize the time-averaged production rate of B using the following stage cost:

$$L_e(x,u) = \frac{k_0 e^{-\frac{E}{RgT}} C_A^2}{N\Delta} \tag{5.25}$$

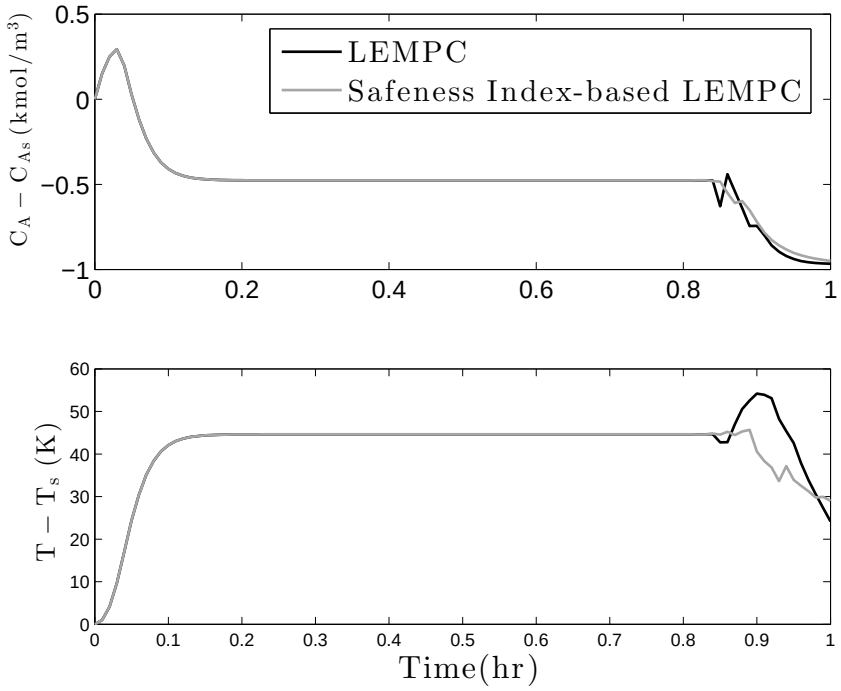

Figure 5.4: The state profiles for the closed-loop CSTR under the LEMPC design of Eq. 5.12 and under the Safeness Index-based LEMPC design of Eq. 5.13 for the initial condition $x_{int}^T = [0\ \frac{kmol}{m^3}\ 0\ K]$.

where the prediction horizon $N = 10$ and the sampling period $\Delta = 0.01\ hr$. In addition, a material constraint that represents the limitation on the amount of reactant material available over a given operating period $t_p = 1.0\ hr$ is described by the following constraint:

$$\frac{1}{t_p}\int_0^{t_p} u_1(\tau)\, d\tau = 0.0\, kmol/m^3. \tag{5.26}$$

The Safeness Index function $S(x)$ for the CSTR is designed as follows so that points in state-space with higher temperatures have larger values of $S(x)$:

$$S(x) = \frac{ax_1 + bx_2}{\max\{ax_1 + bx_2 : V(x) \leq \rho\}} \tag{5.27}$$

where a and b are weighting constants. The value of the Safeness Index $S(x)$ of Eq. 5.27 varies between -1 and 1, where -1 indicates the safest point at which to operate in state-space

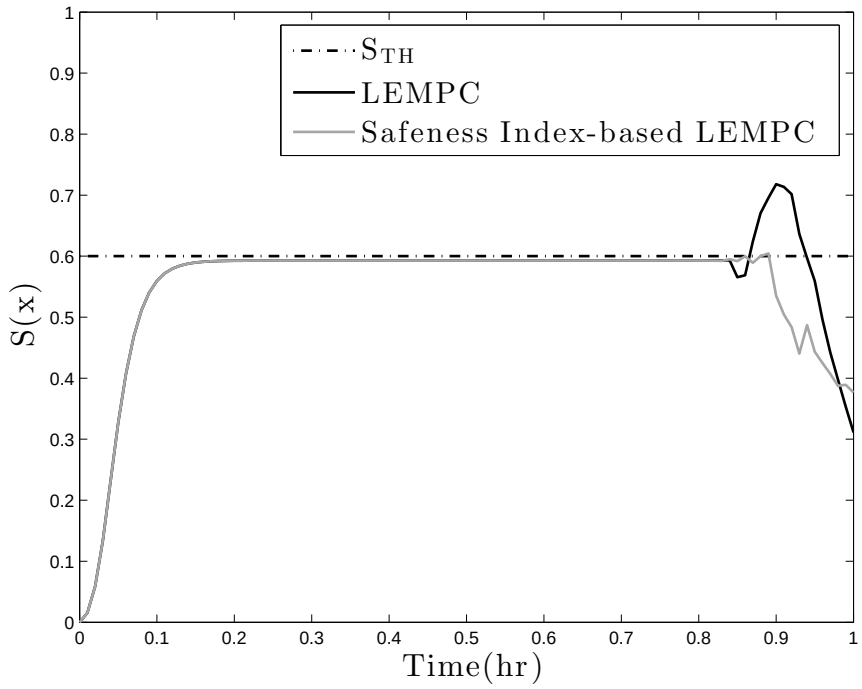

Figure 5.5: The Safeness Index function $S(x)$ for the closed-loop CSTR under the LEMPC design of Eq. 5.12 and under the Safeness Index-based LEMPC design of Eq. 5.13 for the initial condition $x_{int}^T = [0\ \frac{kmol}{m^3}\ 0\ K]$.

and 1 indicates the most unsafe point at which to operate in state-space within the stability region Ω_ρ. In the simulation below, the weighting constants a and b are set to 1 so that the deviation variable form of the temperature (x_2), which can reach several orders of magnitude above the deviation form of C_A (x_1), contributes heavily to the value of the Safeness Index $S(x)$ at a given state. The maximum value of $\max\{ax_1 + bx_2 : V(x) \leq \rho\}$ within the stability region is 74.46. The Safeness Index threshold value S_{TH} is set to 0.6 so that the reactor temperature in deviation form from the steady-state value cannot exceed 47 K (i.e., $x_2 \leq 47\ K$). To guarantee closed-loop stability of the process considered under the controller of Eq. 5.13, a Lyapunov-based controller of the form $h(x) = [h_1(x)\ h_2(x)]^T$ is constructed to estimate the stability region for the Safeness Index-based LEMPC. The inlet concentration control law $h_1(x)$ is set to its steady-state value ($h_1(x) = 0.0\ kmol/m^3$) so that the material constraint of Eq. 5.26 is met. The following feedback

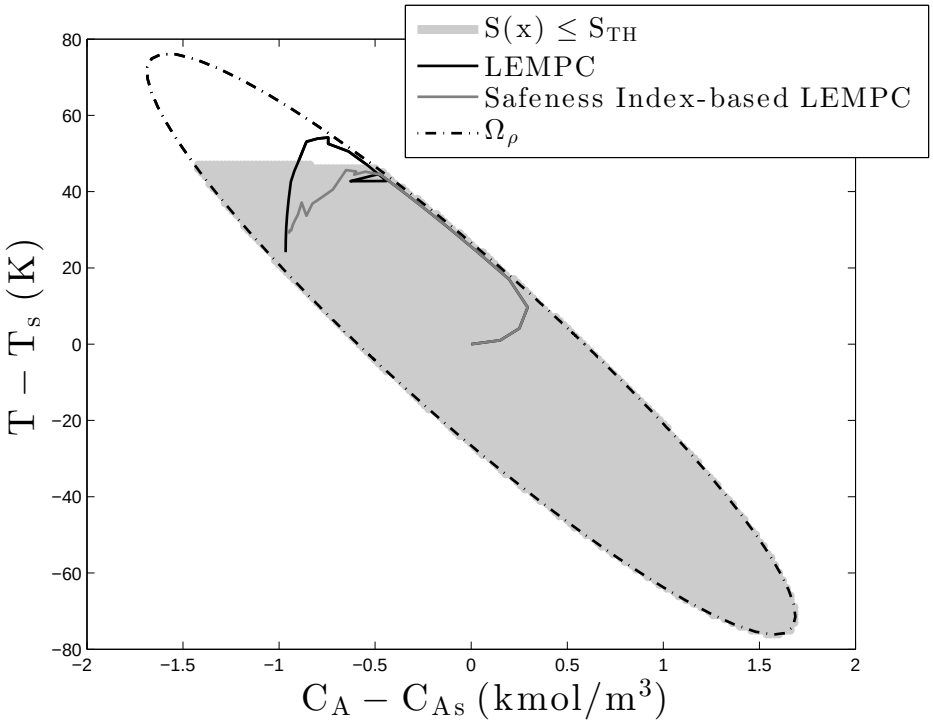

Figure 5.6: The state-space profile for the closed-loop CSTR under the LEMPC design of Eq. 5.12 (black trajectory) and under the Safeness Index-based LEMPC design of Eq. 5.13 (dark gray trajectory) for the initial condition $x_{int}^T = [0\ \frac{kmol}{m^3}\ 0\ K]$.

law (Sontag control law[59]) is utilized for the heat rate u_2:

$$h_2(x) = \begin{cases} -\dfrac{L_{\tilde{f}}V + \sqrt{L_{\tilde{f}}V^2 + L_{g_2}V^4}}{L_{g_2}V}, & \text{if } L_{g_2}V \neq 0 \\ 0, & \text{if } L_{g_2}V = 0 \end{cases} \tag{5.28}$$

where $L_{\tilde{f}}V$ and $L_{g_2}V$ are the Lie derivatives of the Lyapunov function $V(x)$ with respect to the vector fields $\tilde{f}(x)$ and $g_2(x)$ respectively. The control law of Eq. 5.28 is subject to the input constraint (i.e., $|h_2(x)| \leq 5 \times 10^5\ \frac{kJ}{hr}$). Extensive closed-loop simulations were performed under the Lyapunov-based controller $h(x)$ to construct the regions needed in designing stability constraints in the LEMPC of Eq. 5.12. A quadratic Lyapunov function of the form $V(x) = x^T P x$ was utilized to estimate the stability region of the closed-loop system with the following positive definite P

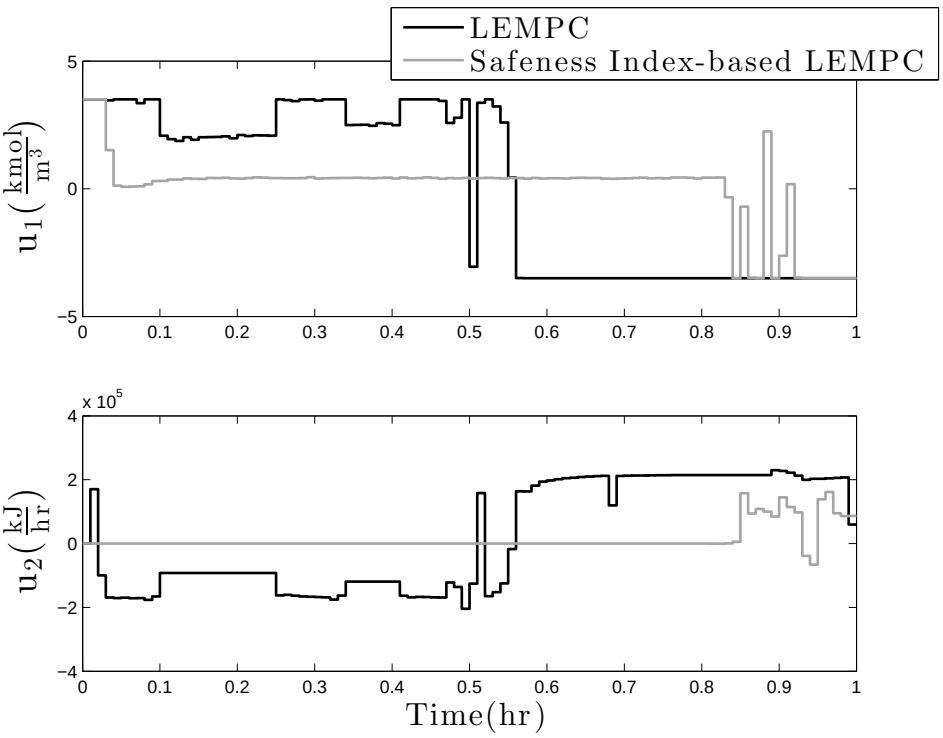

Figure 5.7: Manipulated input profiles for the closed-loop CSTR under the LEMPC design of Eq. 5.12 and under the Safeness Index-based LEMPC design of Eq. 5.13 for the initial condition $x_{int}^T = [0\ \frac{kmol}{m^3}\ 0\ K]$ with bounded process disturbances.

matrix:

$$P = \begin{bmatrix} 1060 & 22 \\ 22 & 0.52 \end{bmatrix}$$

Using this Lyapunov function, ρ was chosen to be 368 and ρ_e was chosen to be 340.

To show that the Safeness Index-based LEMPC is capable of maintaining closed-loop operation within the region where $S(x) \leq S_{TH}$, even when the LEMPC of Eq. 5.12 without the Safeness Index-based constraint would not achieve this, we apply both controllers to the CSTR of Eq. 5.23, where the two optimization problems at each sampling time were solved using the interior-point solver Ipopt.[90] The CSTR was initiated in both cases from the steady-state ($x_{int}^T = [0\ \frac{kmol}{m^3}\ 0\ K]$) where the Safeness Index $S(x)$ equals zero.

Figure 5.3 shows the closed-loop input trajectories for the CSTR under the Safeness Index-based LEMPC scheme and the LEMPC scheme of Eq. 5.12 throughout one hour of operation. The input met the material constraint of Eq. 5.26 under both controllers. Also, the heat rate u_2

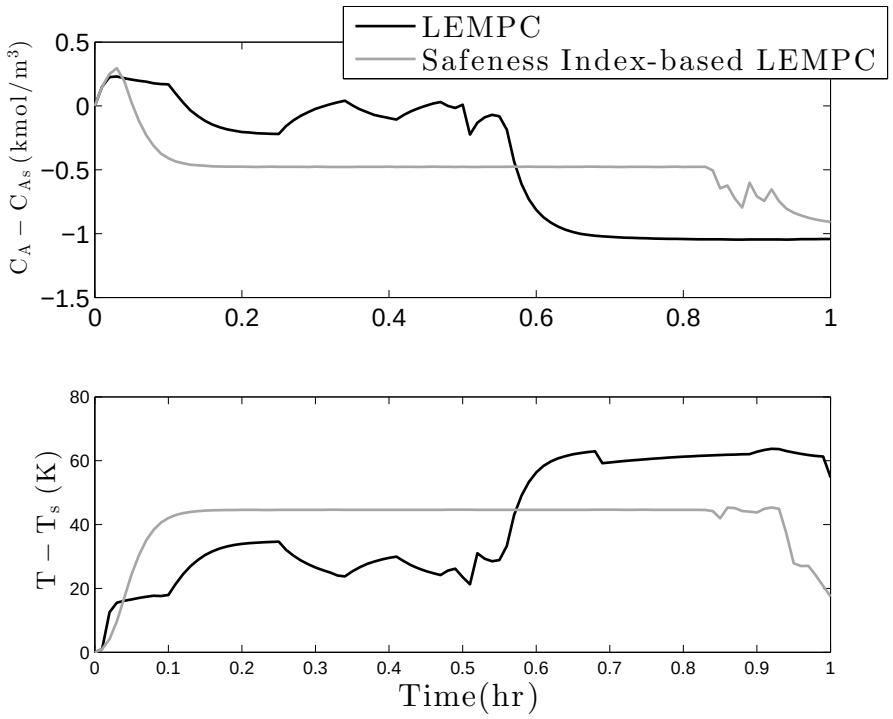

Figure 5.8: The state profiles for the closed-loop CSTR under the LEMPC design of Eq. 5.12 and under the Safeness Index-based LEMPC design of Eq. 5.13 for the initial condition $x_{int}^T = [0\ \frac{kmol}{m^3}\ 0\ K]$ with bounded process disturbances.

of both schemes settled at its steady-state value $u_2 = 0\ \frac{kJ}{hr}$ for close to eighty percent of the one hour of operation, and then deviated from its steady-state value at the end of the simulation so that the other constraints of the formulation (e.g., the material constraint) could be met by the controller while continuing to optimize process economics. Figure 5.4 depicts the trajectories of the reactant concentration and reactor temperature in deviation from the steady-state values ($[x_1\ x_2] = [C_A - C_{As}\ T - T_s]$). From Figures 5.3 and 5.4, it is seen that before the end of the simulation, the behavior of the closed-loop state and the input trajectories under both the Safeness Index-based LEMPC scheme and the LEMPC scheme of Eq. 5.12 are overlapping. This overlap is contributed to by the goal of both LEMPC's to maximize the production rate of B within the stability region over the prediction horizon, which is achieved under both LEMPC's for much of the period of operation by maintaining the closed-loop state at $[x_1\ x_2] = [-0.477\ \frac{kmol}{m^3}\ 44.6\ K]$, which is within the safety zone (i.e., $S(x) = 0.59 \leq 0.6$ where $x = [-0.477\ \frac{kmol}{m^3}\ 44.6\ K]$). At the end of the simulation, the LEMPC's ensure that the material constraint of Eq. 5.26 is met before the

Table 5.1: Parameter values

$T_0 = 300$	K	$F = 5$	$\frac{m^3}{hr}$
$V = 1.0$	m^3	$E = 5 \times 10^4$	$\frac{kJ}{kmol}$
$k_0 = 8.46 \times 10^6$	$\frac{m^3}{kmol hr}$	$\Delta H = -1.15 \times 10^4$	$\frac{kJ}{kmol}$
$C_p = 0.231$	$\frac{kJ}{kgK}$	$R_g = 8.314$	$\frac{kJ}{kmolK}$
$\rho_L = 1000$	$\frac{kg}{m^3}$	$C_{As} = 1.2$	$\frac{kmol}{m^3}$
$T_s = 438$	K	$C_{A0s} = 4$	$\frac{kmol}{m^3}$
$Q_s = 0$	$\frac{kJ}{hr}$		

end of the operating period. When the constraint on $S(x)$ is not imposed, the LEMPC of Eq. 5.12 computes a solution that maximizes the process economics, but leaves the safety region; therefore, the Safeness Index-based LEMPC computes a different trajectory than the LEMPC of Eq. 5.12 at the end of the prediction horizon that meets the material constraint and also maximizes the process economics but subject to the requirement that the closed-loop state cannot leave the safety region. Specifically, Figure 5.4 shows that the closed-loop trajectory of the reactor temperature under the Safeness Index-based LEMPC decreases, while that under the LEMPC design of Eq. 5.12 exceeds the maximum temperature set by the Safeness Index function $S(x)$ because it lacks the Safeness Index-based constraints.

Figure 5.5 further demonstrates that the LEMPC of Eq. 5.12 causes S_{TH} to be exceeded at the end of the operating window by presenting the Safeness Index value $S(x)$ for the LEMPC of Eq. 5.12 and the Safeness Index-based LEMPC over the operating window. Figure 5.6, which displays the state-space trajectories of the reactant concentration and reactor temperature in deviations from the steady-state values ($[x_1\ x_2] = [C_A - C_{As}\ T - T_s]$), also shows this. The closed-loop trajectory under the LEMPC of Eq. 5.12 is seen to leave the safety zone (shaded gray), whereas the closed-loop state under the Safeness Index-based LEMPC never leaves the safety zone.

To illustrate the robustness of the Safeness Index-based LEMPC of Eq. 5.13 and the LEMPC of Eq. 5.12, a bounded disturbance vector $w^T = [w_1\ w_2]$ was added to the right-hand side of Eq. 5.23. The bounded disturbance vector $w^T = [w_1\ w_2]$ corresponds to Gaussian white noise with

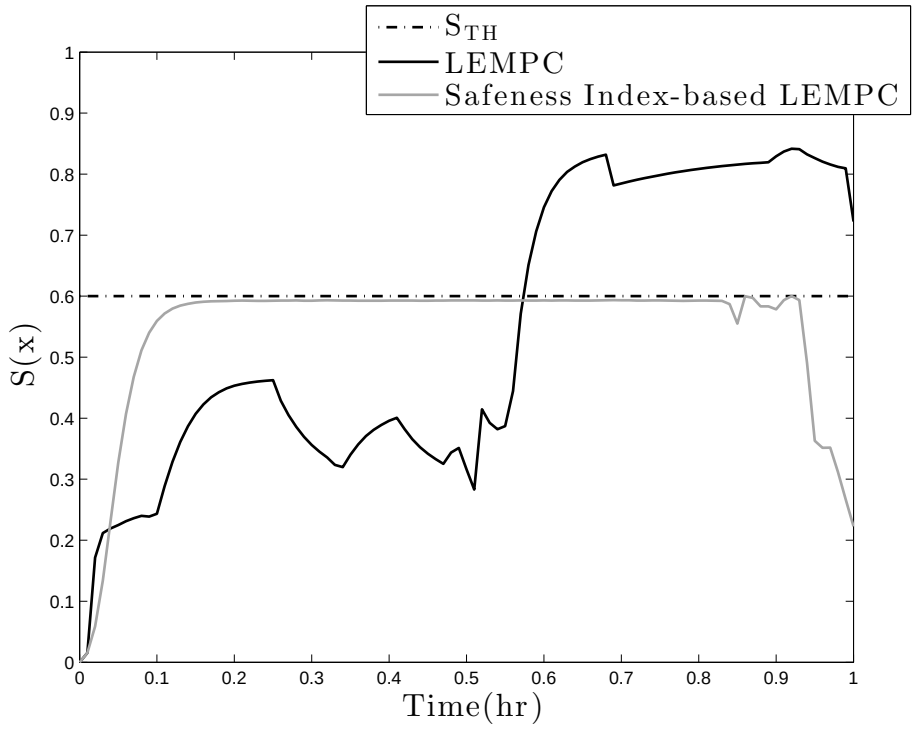

Figure 5.9: The Safeness Index function $S(x)$ for the closed-loop CSTR under the LEMPC design of Eq. 5.12 and under the Safeness Index-based LEMPC design of Eq. 5.13 for the initial condition $x_{int}^T = [0\ \frac{kmol}{m^3}\ 0\ K]$ with bounded process disturbances.

variances $\sigma_1 = 1\ \frac{kmol}{m^3}$ and $\sigma_2 = 20\ K$ with $|w_1| \leq 1\ \frac{kmol}{m^3}$ and $|w_2| \leq 20\ K$. Figures 5.7 and 5.8 show the corresponding manipulated input and state profiles starting from the same initial condition but under bounded process disturbances for both schemes. In the presence of disturbances, the inlet concentration u_1 satisfied the material constraint of Eq. 5.26 under the Safeness Index-based LEMPC and the LEMPC of Eq. 5.12. The heating rate u_2 exhibited similar closed-loop behavior as the case of nominal operation for the Safeness Index-based LEMPC, while u_2 exhibited different closed-loop behavior for the LEMPC in the presence of disturbance. Unlike the case of nominal operation, the closed-loop trajectory of the reactor temperature under the LEMPC exceeds the maximum allowable temperature 47 K for almost half of the operating window due to the disturbance. Figure 5.9 and Figure 5.10 demonstrate that the Safeness Index-based LEMPC was able to maintain the closed-loop state within the safety zone at all times even in the presence of uncertainty while the closed-loop state trajectory under the LEMPC of Eq. 5.12 left the safety zone and never went back to it. It is noted that the two simulations under the different controllers in

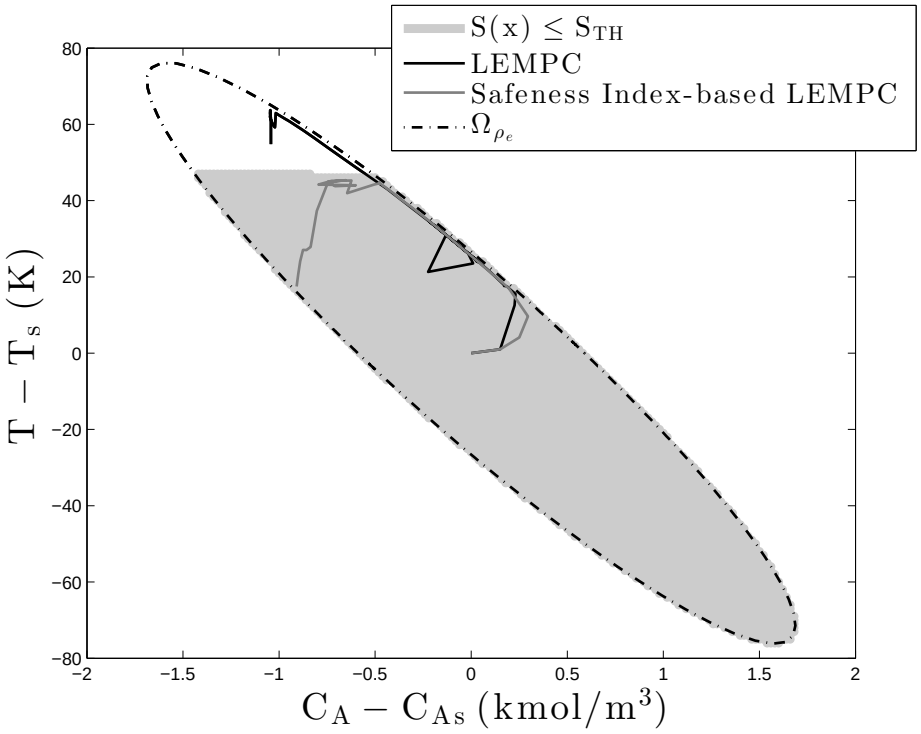

Figure 5.10: The state-space profile for the closed-loop CSTR under the LEMPC design of Eq. 5.12 (black trajectory) and under the Safeness Index-based LEMPC design of Eq. 5.13 (dark gray trajectory) for the initial condition $x_{int}^T = [0\ \frac{kmol}{m^3}\ 0\ K]$ with bounded process disturbances.

Figures 5.7-5.10 had different realizations of the process disturbance than each other at each sampling time (though with the same bounds and standard deviation for the disturbance distribution), which has also contributed to the differences in the trajectories presented.

Remark 5.10 *In the above simulation results, for both nominal process operation (i.e., $w = 0$) and in the presence of disturbance, the Safeness Index-based LEMPC of Eq. 5.13 was feasible at each sampling time when different values of the upper bound of the disturbance were considered. However, in the presence of disturbances that have certain upper bound values (e.g., $\theta_1 = 1\ \frac{kmol}{m^3}$ and $theta_2 = 40\ K$), the classical LEMPC was infeasible towards the end of the operating time period. The proof of closed-loop stability and recursive feasibility of the LEMPC illustrated that for sufficiently small sampling period Δ and sufficiently small upper bound of the disturbance θ, the LEMPC is guaranteed to be feasible at each sampling time. Nevertheless, determining exactly the value of the upper bound of disturbance θ that can ensure feasibility of the LEMPC is difficult*

due to the nonlinearity and nonconvexity of the problem. In addition, incorporating the material constraint of Eq. 5.26 into both the classical LEMPC and the Safeness Index-based LEMPC does not allow guaranteeing a priori closed-loop stability and feasibility of both optimization problems. However, for the value of the upper bounds considered in this simulation ($\theta_1 = 1 \frac{kmol}{m^3}$ and $\theta_2 = 20$ K), both optimization problems were feasible at each sampling time.

5.5 Conclusion

In this chapter, a Safeness Index was developed that can coordinate, for the first time, the control and safety systems within a chemical process plant. Specifically, an approach for defining the functional form of the Safeness Index $S(x)$ was presented, and a methodology of choosing the threshold S_{TH} of the Safeness Index $S(x)$ was given. To demonstrate the use of this Safeness Index within a control system, an LEMPC scheme with a hard Safeness Index-based constraint was presented to integrate feedback control, process safety and process economics within a unified framework. An implementation strategy was developed that is guaranteed, under sufficient conditions, to drive the closed-loop state into the region where the Safeness Index is less than a desired threshold when initiated from any state within the stability region. The proposed method was demonstrated through a chemical process example to be capable of maintaining the closed-loop state within a safe region of operation while maximizing process economics. An illustration of how to define the Safeness Index $S(x)$ and its threshold was given in the context of a non-isothermal continuous stirred tank reactor (CSTR) example where the temperature of the reactor has the largest effect on the safeness of the process.

Chapter 6

Distributed Economic Model Predictive Control with Safeness-Index Based Constraints for Nonlinear Systems

6.1 Introduction

In this chapter, sequential and iterative DEMPC's with Safeness Index-based constraints, and implementation strategies for each, are developed. Sufficient conditions that guarantee closed-loop stability of a nonlinear process operated under these implementation strategies are derived. A catalytic reactor example is used to compare the two distributed controllers with a centralized design in terms of computation time, closed-loop performance, and safety constraints satisfaction. The results of this chapter originally appeared in.[10]

6.2 Preliminaries

6.2.1 Notation

The operator $|\cdot|$ denotes the 2-norm of a vector. The transpose of a vector x is signified by x^T. A level set of a sufficiently smooth, positive definite scalar-valued function $V(x)$ is represented by $\Omega_\rho := \{x \in R^n : V(x) \leq \rho\}$. The operator '/' denotes set subtraction, that is, $A/B := \{x \in R^n : x \in A, x \notin B\}$. The family of piecewise constant, right-continuous functions with a fixed time interval $\Delta \geq 0$ is denoted by $S(\Delta)$. The symbol $\text{diag}(v)$ represents a diagonal matrix which has the components of a vector v as its diagonal elements. A function $\alpha(\cdot) : [0, a) \to [0, \infty)$ belongs to class $\mathscr{K}$ if it is strictly increasing and continuous, and $\alpha(0) = 0$.

6.2.2 Class of Nonlinear Process Systems

We consider nonlinear process systems with the form:

$$\dot{x} = f(x) + \sum_{i=1}^{m} g_i(x)\bar{u_i} + b(x)w \tag{6.1}$$

where $x \in R^{n_x}$, $w \in R^{n_w}$ and $\bar{u_i} \in R^{n_i}$ for $i = 1, \ldots, m$, are the process state vector, disturbance vector and i^{th} manipulated input vector, respectively. Each input vector $\bar{u_i}$ is constrained to be in a nonempty convex set $U_i := \{\bar{u_i} \in R^{n_i} : |\bar{u_i}| \leq \bar{u_i}^{\max}\}$, where $\bar{u_i}^{\max}$ is a bound on the 2-norm of $\bar{u_i}$ resulting from actuator limitations. State measurements are assumed to be available at synchronous time instants $t_k = t_0 + k\Delta$, $k = 0, 1, \ldots$, where Δ is the sampling period and t_0 is the initial time. Bounded disturbances are considered in the sense that $w \in W := \{w \in R^{n_w} : |w| \leq \theta, \theta > 0\}$. The vector functions f, g_i, $i = 1, \ldots, m$, and b are assumed to be locally Lipschitz vector functions of their arguments. The origin is assumed to be an equilibrium point of the unforced nominal (i.e., $w(t) \equiv 0$) system (i.e., $f(0) = 0$, $g_i(0) = 0$, $i = 1, \ldots, m$, and $b(0) = 0$).

6.2.3 Stabilizability Assumption

We consider systems of the form of Eq. 6.1 that are stabilizable in the sense that there exists a locally Lipschitz feedback control law $\bar{h}^T(x) = [\bar{h}_1(x) \ \ldots \ \bar{h}_m(x)]$ with $\bar{h}(0) = 0$ for the nominal closed-loop system of Eq. 6.1 that renders the origin of the nominal system asymptotically stable for all $x \in D \subseteq R^n$, where D is an open neighborhood of the origin, in the sense that there exists a sufficiently smooth Lyapunov function $V(x)$[49,63] for the nominal closed-loop system and class $\mathcal{K}$ functions $\alpha_i(\cdot),\ i = 1,2,3,4$, such that the following inequalities hold for all $x \in D$:

$$\alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|) \tag{6.2a}$$

$$\frac{\partial V(x)}{\partial x}(f(x) + \sum_{i=1}^{m} g_i(x)\bar{h}_i(x)) \leq -\alpha_3(|x|) \tag{6.2b}$$

$$\left|\frac{\partial V(x)}{\partial x}\right| \leq \alpha_4(|x|) \tag{6.2c}$$

$$\bar{h}_i(x) \in U_i,\ i = 1,\ldots,m \tag{6.2d}$$

The stability region of the closed-loop system is taken to be a level set of the Lyapunov function within D where Eq. 6.2 holds, and it is denoted by Ω_ρ.

By the local Lipschitz property assumed for the vector fields f, g_i, $i = 1,\ldots,m$, and b, and the boundedness of both $\bar{u}_i,\ i = 1,\ldots,m$, and w, there exists a positive constant M such that

$$\left| f(x) + \sum_{i=1}^{m} g_i(x)\bar{u}_i + b(x)w \right| \leq M \tag{6.3}$$

for all $x \in \Omega_\rho,\ \bar{u}_i \in U_i,\ i = 1,\ldots,m$, and $w \in W$. In addition, by the smoothness of the Lyapunov function $V(x)$ and the Lipschitz property of f, g_i, $i = 1,\ldots,m$, and b, there exist positive constants $L_x,\ L_{\bar{u}_i},\ i = 1,\ldots,m$, and L_w such that

$$\left|\frac{\partial V}{\partial x} f(x) - \frac{\partial V}{\partial x} f(x')\right| \leq L_x \left|x - x'\right| \tag{6.4}$$

$$\left|\frac{\partial V}{\partial x}g_i(x)-\frac{\partial V}{\partial x}g_i(x')\right|\leq L_{\bar{u_i}}\left|x-x'\right|,\ i=1,\ldots,m \tag{6.5}$$

$$\left|\frac{\partial V}{\partial x}b(x)\right|\leq L_w \tag{6.6}$$

for all $x,x'\in\Omega_\rho$, $\bar{u_i}\in U_i$, $i=1,\ldots,m$, and $w\in W$.

6.3 Centralized Safeness Index-based LEMPC

A Safeness Index (denoted by $S(x)$) that is a function of the process state was developed in.[11] This is a process-specific metric that should be developed with a functional form that causes $S(x)$ to increase as the process state approaches unsafe operating regions in state-space. This allows a threshold S_{TH} to be set on $S(x)$ for use in defining a constraint for an LEMPC that requires predictions of the process state to be maintained within the region where $S(x)\leq S_{TH}$ (the safety

zone)[11] as follows:

$$\max_{u(t)\in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau))\, d\tau \tag{6.7a}$$

$$\text{s.t. } \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{6.7b}$$

$$u(t) \in U,\ \forall\, t \in [t_k, t_{k+N}) \tag{6.7c}$$

$$\tilde{x}(t_k) = x(t_k) \tag{6.7d}$$

$$V(\tilde{x}(t)) \leq \rho_e,\ \forall\, t \in [t_k, t_{k+N})$$
$$\text{if } x(t_k) \in \Omega_{\rho_e} \tag{6.7e}$$

$$S(\tilde{x}(t)) \leq S_{TH},\ \forall\, t \in [t_k, t_{k+N})$$
$$\text{if } S(x(t_k)) \leq S_{TH} \tag{6.7f}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0)$$
$$\leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0),$$
$$\text{if } x(t_k) \in \Omega_\rho / \Omega_{\rho_e} \text{ or } t_k > t_s \text{ or } S(x(t_k)) > S_{TH} \tag{6.7g}$$

where the input trajectory $u(t)$ is the decision variable of the optimization problem of Eq. 6.7 over the prediction horizon $N\Delta$. This control scheme seeks to maintain safe operation of a class of nonlinear systems while maximizing the economic measure $L_e(x(t), u(t))$ (Eq. 6.7a) that defines the stage cost, subject to input constraints (Eq. 6.7c) and a nominal process model (Eq. 6.7b) initialized with a state measurement at the current sampling time t_k (Eq. 6.7d). The notation t_s denotes the time after which it is desired to apply the constraint of Eq. 6.7g. The predicted state trajectory $\tilde{x}(t)$ is maintained within Ω_{ρ_e} throughout the prediction horizon by the constraint of Eq. 6.7e when $x(t_k) \in \Omega_{\rho_e}$. The region Ω_{ρ_e} is chosen such that if the measured state $x(t_k)$ is within Ω_{ρ_e}, then $x(t_{k+1})$ is still within Ω_{ρ_e} even in the presence of uncertainty. The constraint of Eq. 6.7f maintains the predicted closed-loop state within the safety zone throughout the prediction horizon when $S(x(t_k)) \leq S_{TH}$. The safety zone is assumed to contain the origin of the system of Eq. 6.1 in its interior. The contractive constraint of Eq. 6.7g guarantees that the calculated control actions

will decrease the value of the Lyapunov function between t_k and t_{k+1} when this constraint is applied (i.e., $x(t_k) \in \Omega_\rho / \Omega_{\rho_e}$, $t_k > t_s$, or $S(x(t_k)) > S_{TH}$).

When the constraint of Eq. 6.7f is not applied (i.e., $S(x(t_k)) > S_{TH}$), $\bar{h}(\tilde{x}(t_q)), \forall\, t \in [t_q, t_{q+1}), q = k, \ldots, k+N-1$, is a feasible solution to the Safeness Index-based LEMPC optimization problem.[43] However, because the safety zone is not required to take a certain shape (e.g., it is not required to be a Lyapunov level set), $\bar{h}(\tilde{x}(t_q)), \forall\, t \in [t_q, t_{q+1}), q = k, \ldots, k+N-1$, does not necessarily meet this constraint and therefore, the centralized Safeness Index-based LEMPC may become infeasible when the constraint of Eq. 6.7f is applied.

Remark 6.1 *In this chapter, we focus on distributed LEMPC designs with Safeness Index-based constraints for the case that S_{TH} is not a hard threshold (i.e., when $S(x) > S_{TH}$, that does not necessarily mean that the process requires operator intervention, but may instead reflect that the process should avoid operating in a region where $S(x) > S_{TH}$ for long periods of time). The case where S_{TH} is a hard threshold can be handled by choosing $S(x)$ as a Lyapunov function and selecting S_{TH} such that the closed-loop state cannot leave a safe operating region within a sampling period if S_{TH} is the upper bound on $S(x)$ in Eq. 6.7f. Such a design would be similar to the safety-based LEMPC design for which a distributed control architecture has already been developed in*[9] *and therefore will not be considered here.*

6.4 Distributed Safeness Index-based LEMPC design

The computation time required to solve the centralized Safeness Index-based LEMPC of the prior section may be significant with the process model and constraints of a large-scale industrial nonlinear process system. Therefore, the problem may not be solved to optimality within a short sampling period, which prevents the optimization problem from being solved frequently with new state measurements. However, frequent feedback of the process state can be beneficial for enhancing process safety under this control law because the safety zone is not necessarily an invariant set under the Safeness Index-based LEMPC design, and the controller is made aware that the state has exited

the safety zone (so that it can compute control actions guaranteed to drive the state back into the safety zone in finite time) through feedback of the process state (Eq. 6.7g). Moreover, this LEMPC design may be applied in practice to processes for which the upper bound on the disturbance is estimated but not known (though that is not the theoretical consideration in this chapter), and in such cases, more frequent feedback may aid in preventing the closed-loop state from exiting the safety zone during a sampling period if a large disturbance potentially greater than the expected bound affects the process. To obtain Safeness Index-based controllers with reduced computation time (allowing more frequent feedback) compared to the centralized design, this chapter develops two distributed (sequential and iterative) Safeness Index-based LEMPC designs. Sufficient conditions that guarantee closed-loop stability of a nonlinear process under the implementation strategies of the two distributed LEMPC (DLEMPC) designs with Safeness Index-based constraints are given.

6.4.1 Safeness Index-based Sequential DLEMPC

The first distributed control scheme considered is a sequential Safeness Index-based DLEMPC (termed Safeness Index-S-DLEMPC) design where each of m controllers solves for a different subset of the set of all control actions. The j^{th} controller solves for the n_j control actions in vector $\bar{u}_j$ out of the total $n_{tot} = \sum_{i=1}^{m} n_i$ available control actions while it assumes values of the remaining $n_{tot} - n_j$ manipulated inputs. In the Safeness Index-S-DLEMPC design, the m controllers form a hierarchy connected using a one-directional communication network and are evaluated in sequence (i.e., the first LEMPC in the hierarchy calculates $\bar{u}_1$, the second LEMPC receives the computed value of $\bar{u}_1$ and calculates $\bar{u}_2$, and so on). The j^{th} controller, $j \in \{1,\ldots,m\}$, in the hierarchy (Safeness Index-S-DLEMPC j) solves only for $\bar{u}_j$. It assumes that $\bar{u}_z$, $z = 1,\ldots,j-1$, are the optimal values of these control actions from the controllers higher up in the hierarchy, and assumes that $\bar{u}_z = \bar{h}_z(\tilde{x}(t_q))$, $\forall\, t \in [t_q, t_{q+1})$, $q = k,\ldots,k+N-1$, for $z = j+1,\ldots,m$. The $j-th$ Safeness

Index-S-DLEMPC solves the following optimization problem:

$$\max_{\bar{u}_j \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}^j(\tau), \bar{u}_1(\tau), \ldots, \bar{u}_m(\tau)) d\tau \tag{6.8a}$$

$$\text{s.t. } \dot{\tilde{x}}^j(t) = f(\tilde{x}^j(t)) + \sum_{i=1}^{m} g_i(\tilde{x}^j(t))\bar{u}_i(t) \tag{6.8b}$$

$$\bar{u}_j(t) \in U_j, \ \forall\, t \in [t_k, t_{k+N}) \tag{6.8c}$$

$$\bar{u}_r(t) = \bar{h}_r(\tilde{x}^j(t_{k+q})), \ r = j+1, \ldots, m, \tag{6.8d}$$

$$\forall\, t \in [t_{k+q}, t_{k+q+1}), \ q = 0, \ldots, N-1$$

$$\bar{u}_p(t) = \bar{u}_p^*(t|t_k), \tag{6.8e}$$

$$p = 1, \ldots, j-1, \ t \in [t_k, t_{k+N})$$

$$\tilde{x}^j(t_k) = x(t_k) \tag{6.8f}$$

$$V(\tilde{x}^j(t)) \leq \rho_e, \ \forall\, t \in [t_k, t_{k+N}) \tag{6.8g}$$

$$\text{if } x(t_k) \in \Omega_{\rho_e}$$

$$S(\tilde{x}^j(t)) \leq S_{TH}, \ \forall\, t \in [t_k, t_{k+N}) \tag{6.8h}$$

$$\text{if } S(x(t_k)) \leq S_{TH}$$

$$\frac{\partial V(x(t_k))}{\partial x}\left(\sum_{i=1}^{m} g_i(x(t_k))\bar{u}_i(t_k)\right) \leq \frac{\partial V(x(t_k))}{\partial x}\left(\sum_{i=1}^{m} g_i(x(t_k))\bar{h}_i(x(t_k))\right), \tag{6.8i}$$

$$\text{if } x(t_k) \in \Omega_\rho / \Omega_{\rho_e} \text{ or } t_k > t_s \text{ or } S(x(t_k)) > S_{TH}$$

where $\tilde{x}^j(t)$ denotes the predicted state trajectory under Safeness Index-S-DLEMPC j. The constraint of Eq. 6.8e sets the trajectory of each $\bar{u}_p$, $p = 1, \ldots, j-1$, to the optimal trajectory (denoted by $\bar{u}_p^*(t|t_k)$, $t \in [t_k, t_{k+N})$) calculated by Safeness Index-S-DLEMPC p, $p = 1, \ldots, j-1$. The values of the inputs $\bar{u}_r$, $r = j+1, \ldots, m$, that will be calculated by Safeness Index-S-DLEMPC's later in the sequence of m controllers are set by the constraint of Eq. 6.8d to the corresponding elements of $\bar{h}(x)$ applied in a sample-and-hold fashion. The other constraints of the optimization problem of

Eq. 6.8 follow those in Eq. 6.7.

The manner in which the n_{tot} inputs are partitioned between the various $\bar{u}_j$ and the order in which the various $\bar{u}_j$ are computed in the hierarchy of distributed controllers can impact whether each of the m controllers in the hierarchy is feasible. Specifically, when Eq. 6.8h is not applied (i.e., $S(x(t_k)) > S_{TH}$), $\bar{u}_j = \bar{h}_j(\tilde{x}(t_q))$, $\forall\ t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$, is a feasible control action for Safeness Index-S-DLEMPC j. However, the region where $S(x) \leq S_{TH}$ is not required to take a specific shape, so when Eq. 6.8h is applied, there is no guarantee that any control action within the input bounds can satisfy this constraint (whether or not constraints such as Eqs. 6.8g and/or 6.8i are simultaneously applied). This means that the j^{th} Safeness Index-S-DLEMPC will have a feasible solution when the constraint of Eq. 6.8h is applied only if there exists a $\bar{u}_j$ that, when $\bar{u}_p(t) = \bar{u}_p^*(t|t_k)$, $p = 1, \ldots, j-1$, $t \in [t_k, t_{k+N})$, and $\bar{u}_r(t) = \bar{h}_r(\tilde{x}^j(t_{k+q}))$, $r = j+1, \ldots, m$, $\forall\ t \in [t_{k+q}, t_{k+q+1})$, $q = 0, \ldots, N-1$, the state predictions are maintained within the safety zone. Furthermore, if the control actions calculated by Safeness Index-S-DLEMPC 1 ensure that $S(\tilde{x}^1) \leq S_{TH}$ throughout the prediction horizon (i.e., Safeness Index-S-DLEMPC 1 is feasible even when Eq. 6.8h is applied), then Safeness Index-S-DLEMPC 2 to Safeness Index-S-DLEMPC m will be feasible as well because a feasible solution to Safeness Index-S-DLEMPC j is a feasible solution to Safeness Index-S-DLEMPC $j+1$. Hence, grouping inputs that have a large effect on the magnitude of $S(x)$ (and thus provide significant flexibility for adjusting its value throughout the prediction horizon to seek to maintain the state predictions within the safety zone) together within $\bar{u}_1$ may enable the constraint of Eq. 6.8h to be feasible more regularly in Safeness Index-S-DLEMPC 1 than if inputs with less impact on $S(x)$ were computed by this controller. This would allow the set of m distributed controllers to be feasible more regularly as well (since all are feasible if Safeness Index-S-DLEMPC 1 is feasible). Furthermore, other process constraints beyond those presented in Eq. 6.8 may be added to the Safeness Index-S-DLEMPC's (e.g., constraints on the time-averaged value of certain inputs or products of inputs due to physical constraints on the process; an example of this is shown in the section "Application to a Chemical Process Example," where the product of two inputs represents the total amount of reactant available

to a process which is limited in a given period of time), and input partitioning may impact feasibility of these constraints as well. For example, if a constraint on the product of two inputs is present, it may be desirable to solve for both inputs in the same Safeness Index-S-DLEMPC if it is likely that the constraint will be infeasible if such flexibility in satisfying the constraint is not provided. Process economics may be impacted by the manner in which the inputs are partitioned (e.g., as the number of control actions n_j determined by Safeness Index-S-DLEMPC j is decreased due to an increasing magnitude of m, Safeness Index-S-DLEMPC j may have less flexibility to maximize process economic performance). Computation time is also affected by input partitioning (e.g., it may increase for Safeness Index-S-DLEMPC j if n_j is increased to provide the LEMPC with greater flexibility in control action selection for feasibility and/or economics reasons). Thus, an appropriate partitioning of inputs may be based on trade-offs between feasibility, economics, and computation time considerations. This approach for partitioning inputs may be complemented by other methods of input partitioning (see, e.g.,[29,47]), though the partitions resulting from alternative methods should be evaluated from the feasibility standpoint discussed before being used.

A schematic of the Safeness Index-S-DLEMPC architecture is depicted in Figure 6.1. An implementation issue for the Safeness Index-S-DLEMPC design is that, when Safeness Index-S-DLEMPC 1 is infeasible when the constraint of Eq. 6.8h is applied, no feasible solution to Safeness Index-S-DLEMPC 1 is available to be sent to Safeness Index-S-DLEMPC 2 to m. Safeness Index-S-DLEMPC 2 to m cannot then be solved to obtain $u_i^*(t_k|t_k)$, $i = 1,\ldots,m$, to apply to the process; in such cases, we require that the explicit stabilizing controller $\bar{h}_i(x(t_k))$, $i = 1,\ldots,m$, be applied to the plant because $\bar{h}(x(t_k))$ is guaranteed to maintain the closed-loop state in Ω_ρ throughout a sampling period.[72] This implementation strategy for the Safeness Index-S-DLEMPC design is summarized as follows:

1. At t_k, the m Safeness Index-S-DLEMPC's receive a measurement of the current state $x(t_k)$ from the sensors. Go to Step 2.

2. Solve Safeness Index-S-DLEMPC 1. If the Safeness Index-S-DLEMPC 1 optimization problem is feasible, go to Step 2a. Else, go to Step 2b.

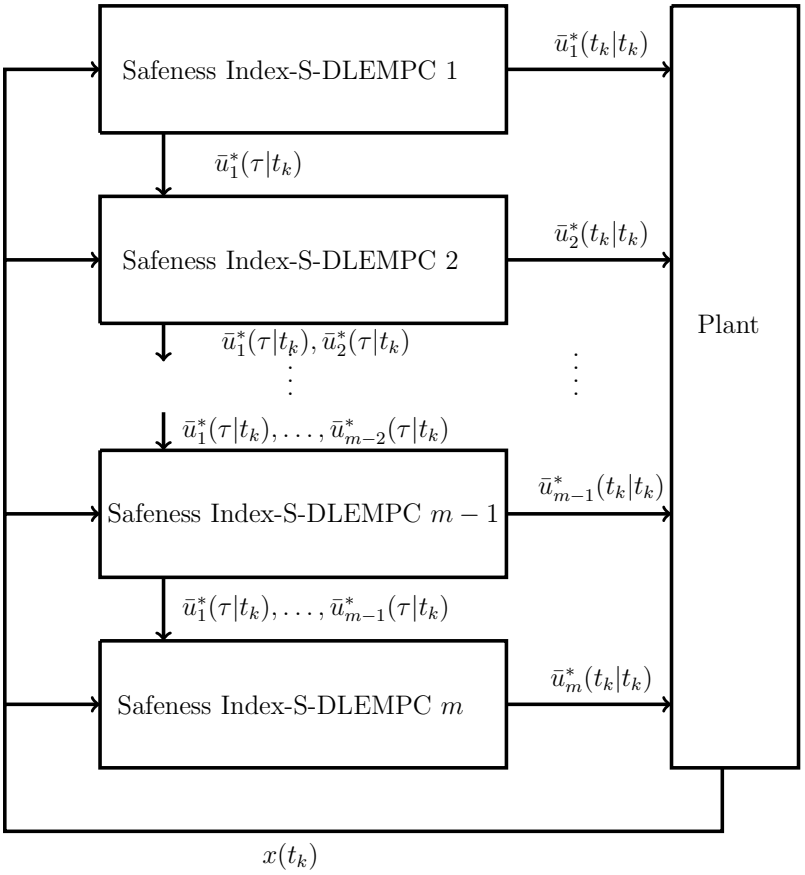

Figure 6.1: Block diagram of the Safeness Index-S-DLEMPC scheme.

(a) Safeness Index-S-DLEMPC 1 sends $\bar{u}_1^*(\tau|t_k)$, $\tau \in [t_k, t_{k+N})$, to Safeness Index-S-DLEMPC 2. Go to Step 3 ($j = 2$).

(b) Apply $\bar{u}_i(t_k) = \bar{h}_i(x(t_k))$, $i = 1, \ldots, m$, to the plant. Go to Step 6.

3. Solve Safeness Index-S-DLEMPC j. If $j < m$, go to Step 4. If $j = m$, go to Step 5.

4. Send $\bar{u}_p^*(\tau|t_k)$, $\tau \in [t_k, t_{k+N})$, $p = 1, \ldots, j$, to Safeness Index-S-DLEMPC $j+1$. Go to Step 3 ($j \leftarrow j+1$).

5. The m Safeness Index-S-DLEMPC's send the optimal solutions $u_i^*(t_k|t_k)$, $i = 1, \ldots, m$, for the first sampling period of the prediction horizon to the actuators to be implemented on the process. Go to Step 6.

6. When a new state measurement is received at t_{k+1}, go to Step 1 ($k \leftarrow k+1$).

Remark 6.2 *The partitioning of the inputs based on feasibility is not intended to make the m Safeness Index-S-DLEMPC's feasible at each sampling time (e.g., when the centralized Safeness Index-based LEMPC of Eq. 6.7 would be infeasible at t_k, there is no partitioning of the inputs that would be able to make Safeness Index-S-DLEMPC 1 to m feasible). Appropriate partitioning is intended to prevent the distributed controllers from frequently becoming infeasible when the centralized design would not have been.*

6.4.2 Feasibility and Closed-Loop Stability Analysis for the Safeness Index-S-DLEMPC Implementation Strategy

In this subsection, we prove closed-loop stability of a nonlinear process operated under the Safeness Index-S-DLEMPC implementation strategy. To proceed with this analysis, we present a proposition that illustrates the closed-loop stability properties of the Lyapunov-based controller used for the Safeness Index-S-DLEMPC constraint design.

Proposition 6.1 (c.f.[72]) *Consider the trajectory $\hat{x}(t)$ of the system of Eq. 6.1 in closed-loop under a controller $\bar{h}(x)$, which satisfies the conditions of Eq. 6.2, obtained by solving recursively:*

$$\dot{\hat{x}}(t) = f(\hat{x}(t)) + \sum_{i=1}^{m} g_i(\hat{x}(t))\bar{h}_i(\hat{x}(t_k)) + b(\hat{x}(t))w(t) \tag{6.9}$$

where $t \in [t_k, t_{k+1})$ with $k = 0, 1, \ldots$. Let $\Delta, \varepsilon_w > 0$ and $\rho > \rho_s > 0$ satisfy:

$$-\alpha_3(\alpha_2^{-1}(\rho_s)) + (L_x + \sum_{i=1}^{m} L_{\bar{u}_i}\bar{u}_i^{\max})M\Delta + L_w\theta \leq -\varepsilon_w/\Delta. \tag{6.10}$$

Then, if $\hat{x}(t_0) \in \Omega_\rho$ and $\rho_{\min} < \rho$ where

$$\rho_{\min} = \max\{V(x(t+\Delta)) : V(x(t)) \leq \rho_s\}, \tag{6.11}$$

the following inequality holds:

$$V(\hat{x}(t_k)) \leq \max\{V(\hat{x}(t_0)) - k\varepsilon_w, \rho_{\min}\}. \tag{6.12}$$

We note that $\rho_{\min}$ in Proposition 6.1 is defined without reference to a specific controller such as $\bar{h}(x)$, but rather as the maximum value that $V(x)$ can take in a time period Δ if $V(x(t)) \leq \rho_s$ at the beginning of this time period, given Δ and the constraints. Proposition 6.1 guarantees that with a sufficiently small sampling period and bound on the disturbance (i.e., Eq. 6.10 holds), the magnitude of $V(x)$ decreases throughout a sampling period for the system of Eq. 6.1 under $\bar{h}(x)$ when $\hat{x}(t_k) \in \Omega_\rho / \Omega_{\rho_s}$, and when $\hat{x}(t_k) \in \Omega_{\rho_s}$, then $\hat{x}(t) \in \Omega_{\rho_{\min}}$, $\forall\, t \in [t_k, t_{k+1})$.

Two additional propositions that will be used in the closed-loop stability analysis of a nonlinear process under the Safeness Index-S-DLEMPC implementation strategy are now introduced. The first bounds the norm of the difference between the trajectories of the nominal and perturbed (i.e., $w(t) \not\equiv 0$) systems when initiated from the same initial condition. The second bounds the difference in the Lyapunov function value at different locations in the stability region.

Proposition 6.2 (c.f.[43,67]) *Consider the systems*

$$\begin{aligned} \dot{x}_a(t) &= f(x_a(t)) + \textstyle\sum_{i=1}^{m} g_i(x_a(t))\bar{u}_i(t) + b(x_a(t))w(t) \\ \dot{x}_b(t) &= f(x_b(t)) + \textstyle\sum_{i=1}^{m} g_i(x_b(t))\bar{u}_i(t) \end{aligned} \tag{6.13}$$

with initial states $x_a(t_0) = x_b(t_0) \in \Omega_\rho$. There exists a $\mathscr{K}$ function $f_W(\cdot)$ such that

$$|x_a(t) - x_b(t)| \leq f_W(t - t_0), \tag{6.14}$$

for all $x_a(t), x_b(t) \in \Omega_\rho$ and all $w(t) \in W$ with

$$f_W(\tau) = \frac{L'_w \theta}{L'_x}(e^{L'_x \tau} - 1). \tag{6.15}$$

where L'_w and L'_x are positive constants.

Proposition 6.3 (c.f.[43,67]) *Consider the Lyapunov function $V(\cdot)$ of the system of Eq. 6.1. There exists a quadratic function $f_V(\cdot)$ such that*

$$V(x) \leq V(\hat{x}) + f_V(|x-\hat{x}|) \tag{6.16}$$

for all $x, \hat{x} \in \Omega_\rho$ with

$$f_V(s) = \alpha_4(\alpha_1^{-1}(\rho))s + M_v s^2 \tag{6.17}$$

where M_v is a positive constant.

Theorem 6.1 below provides sufficient conditions which guarantee closed-loop stability of the system of Eq. 6.1 under the Safeness Index-S-DLEMPC implementation strategy.

Theorem 6.1 *Consider the system of Eq. 6.1 in closed-loop under the implementation strategy (Steps 1-6) of the Safeness Index-S-DLEMPC based on a controller $\bar{h}(x)$ that satisfies the conditions of Eq. 6.2. Let $\varepsilon_w > 0$, $\Delta > 0$, $\rho > \rho_e > \rho_s > 0$ satisfy*

$$\rho_e \leq \rho - f_V(f_W(\Delta)) \tag{6.18}$$

and Eq. 6.10. If $x(t_0) \in \Omega_\rho$, $\rho_{\min} \leq \rho_e$ and $N \geq 1$ where $\rho_{\min}$ is defined as in Eq. 6.11 and where the compact set $\Omega_{\rho_{\min}}$ satisfies

$$\Omega_{\rho_{\min}} \subseteq \{x \in \Omega_\rho \ : \ S(x) \leq S_{TH}\}, \tag{6.19}$$

then the closed-loop state $x(t)$ of Eq. 6.1 is guaranteed to enter the safety zone in finite time when $x(t_0) \in \Omega_\rho$, to be bounded within Ω_ρ at all times, and to be ultimately bounded in $\Omega_{\rho_{\min}}$.

Proof 6.1 *The proof of Theorem 1 is given in two parts. The first part is the proof of the existence of an input trajectory with characterizable properties for the process of Eq. 6.1 operated under Steps 1-6 of the Safeness Index-S-DLEMPC implementation strategy when $x(t_0) \in \Omega_\rho$. The proof*

of the three results of Theorem 1 given these characterizable properties is provided in the second part of the proof of Theorem 1.

Part 1: Based on the implementation strategy of the Safeness Index-S-DLEMPC, in a given sampling period, either: 1) Safeness Index-S-DLEMPC 1 is a feasible optimization problem and $\overline{u}_1^*(\tau|t_k)$, $\tau \in [t_k, t_{k+N})$, *is communicated to Safeness Index-S-DLEMPC 2, or 2) Safeness Index-S-DLEMPC 1 is not feasible and* $\overline{h}_i(x(t_k))$ *for* $i = 1,\ldots,m$, *is applied to the process for* $t \in [t_k, t_{k+1})$. *In the case that Safeness Index-S-DLEMPC 1 is feasible, Safeness Index-S-DLEMPC's* 2 *to m are guaranteed to be feasible. This is because if Safeness Index-S-DLEMPC* j *is feasible with the input trajectories defined by* $\overline{u}_j^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $\overline{u}_p(t) = \overline{u}_p^*(t|t_k)$, $p = 1,\ldots,j-1$, $t \in [t_k, t_{k+N})$, *and* $\overline{u}_r(t) = \overline{h}_r(\tilde{x}^j(t_{k+q}))$, $r = j+1,\ldots,m$, $\forall\ t \in [t_{k+q}, t_{k+q+1})$, $q = 0,\ldots,N-1$, *then in Safeness Index-S-DLEMPC* $j+1$, *which solves for* $\overline{u}_{j+1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, *but sets the other inputs according to the constraints of Eqs. 6.8d-6.8e (which forces all inputs except* $\overline{u}_{j+1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, *to take the same values as they had in the feasible solution returned by Safeness Index-S-DLEMPC* j*), the trajectory of* $\overline{u}_{j+1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, *that was feasible for Safeness Index-S-DLEMPC* j *(i.e.,* $\overline{u}_{j+1}^*(t|t_k) = \overline{h}_{j+1}(\tilde{x}(t_q))$, $\forall\ t \in [t_q, t_{q+1})$, $q = k,\ldots,k+N-1$*) is feasible for Safeness Index-S-DLEMPC* $j+1$. *When* $\overline{u}_{j+1}^*(t|t_k) = \overline{h}_{j+1}(\tilde{x}(t_q))$, $\forall\ t \in [t_q, t_{q+1})$, $q = k,\ldots,k+N-1$, *is applied with the input trajectories of Eqs. 6.8d-6.8e, the state predictions of Eq. 6.8b for Safeness Index-S-DLEMPC's* j *and* $j+1$ *are initiated from the same initial condition (Eq. 6.8f) and have the same input trajectories. We assume that the local Lipschitz property for vector functions* f, g *and* b *allows them to be constructed such that since* $x(t) \in \Omega_\rho$ *for all times (as will be demonstrated in Part 2 of this proof), Eq. 6.8b in Safeness Index-S-DLEMPC's* j *and* $j+1$ *has the same unique solution throughout the prediction horizon when the same input trajectories are applied;*[49] *therefore, if such trajectories meet the constraints of Eqs. 6.8g-6.8i in Safeness Index-S-DLEMPC* j, *they will also meet them in Safeness Index-S-DLEMPC* $j+1$. *The only constraint in Eq. 6.8 that is enforced in Safeness Index-S-DLEMPC* $j+1$ *that is not enforced in Safeness Index-S-DLEMPC* j *is Eq. 6.8c (in Safeness Index-S-DLEMPC* j, *it is enforced on* $\overline{u}_j$, *whereas in Safeness Index-S-DLEMPC* $j+1$, *it is enforced on* $\overline{u}_{j+1}$*). By Eq. 6.2, however,* $\overline{u}_{j+1}^*(t|t_k) = \overline{h}_{j+1}(\tilde{x}(t_q))$,

$\forall\ t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$, *satisfies this constraint as well, showing that this trajectory fully satisfies all constraints of Safeness Index-S-DLEMPC* $j+1$ *if Safeness Index-S-DLEMPC* j *was feasible. Because Safeness Index-S-DLEMPC 1 is feasible, Safeness Index-S-DLEMPC's 2 to m are therefore feasible by induction. When a feasible solution to Safeness Index-S-DLEMPC's 1 to m is obtained, Eqs. 6.8b-6.8i are satisfied in Safeness Index-S-DLEMPC m for the set of implemented control actions* $\overline{u}_i^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $i = 1, \ldots, m$, *and thus the set of implemented control actions has characterizable properties. When Safeness Index-S-DLEMPC 1 is not feasible and* $\overline{h}(x(t_k))$ *is applied, the conditions of Proposition 6.1 hold. Thus, the control actions applied to the process according to the Safeness Index-S-DLEMPC implementation strategy throughout any sampling period have characterizable properties that can be used to analyze closed-loop stability of a nonlinear process under these control actions.*

Part 2: We now prove the results of Theorem 6.1. To prove that if $S(x(t_k)) > S_{TH}$ *and* $x(t_0) \in \Omega_\rho$, *then the Safeness Index-S-DLEMPC implementation strategy will drive the closed-loop state into the safety zone in finite time, we demonstrate that either a feasible solution to all m distributed controllers of the Safeness Index-S-DLEMPC design or* $\overline{h}(x(t_k))$ *will drive the closed-loop state toward the set* $\Omega_{\rho_{\min}}$ *(which is within the safety zone from Eq. 6.19) throughout a given sampling period. When all m Safeness Index-S-DLEMPC's are feasible at a given sampling time (which follows if Safeness Index-S-DLEMPC 1 is feasible), the set of control actions* $\overline{u}_i^*(t_k|t_k)$, $i = 1, \ldots, m$, *that are applied to the process satisfy the constraints of Safeness Index-S-DLEMPC m (the last controller in the hierarchy). Specifically, when* $S(x(t_k)) > S_{TH}$, *from the contractive constraint of Eq. 6.8i and Eq. 6.2b, we obtain:*

$$\frac{\partial V(x(t_k))}{\partial x}(f(x(t_k)) + \sum_{i=1}^{m} g_i(x(t_k))\overline{u}_i^*(t_k|t_k)) \leq$$
$$\frac{\partial V(x(t_k))}{\partial x}(f(x(t_k)) + \sum_{i=1}^{m} g_i(x(t_k))\overline{h}_i(x(t_k))) \tag{6.20a}$$
$$\leq -\alpha_3(|x(t_k)|) \tag{6.20b}$$

The time derivative of the Lyapunov function along the state trajectory $x(t)$ *under* $\overline{u}_i^*(t_k|t_k)$,

$i = 1, \ldots, m$, *for* $t \in [t_k, t_{k+1})$, *is:*

$$\dot{V}(x(t)) = \frac{\partial V(x(t))}{\partial x}\left(f(x(t)) + \sum_{i=1}^{m} g_i(x(t))\bar{u}_i^*(t_k|t_k) + b(x(t))w(t) \right) \tag{6.21}$$

Adding and subtracting $\frac{\partial V(x(t_k))}{\partial x}(f(x(t_k)) + \sum_{i=1}^{m} g_i(x(t_k))\bar{u}_i^*(t_k|t_k))$ *to/from Eq. 6.21, we obtain the following inequality by utilizing Eq. 6.20, the Lipschitz properties in Eqs. 6.4-6.6, and the disturbance bound* $|w| \leq \theta$*:*

$$\dot{V}(x(t)) \leq -\alpha_3(|x(t_k)|) + \left(L_x + \sum_{i=1}^{m} L_{\bar{u}_i}\bar{u}_i^*(t_k|t_k) \right)|x(t) - x(t_k)| + L_w\theta \tag{6.22}$$

From the continuity of $x(t)$ *and Eq. 6.3, the following bound holds for all* $t \in [t_k, t_{k+1})$*:*

$$|x(t) - x(t_k)| \leq M\Delta \tag{6.23}$$

Because $S(x(t_k)) > S_{TH}$*, it follows from Eqs. 6.11 and 6.19 that* $x(t_k) \in \Omega_\rho / \Omega_{\rho_s}$*. In addition, since Eqs. 6.22-6.23 and the bounds on* $\bar{u}_i,\ i = 1, \ldots, m$*, also hold, the following bound on* $\dot{V}(x(t))$ *can be written for* $t \in [t_k, t_{k+1})$*:*

$$\dot{V}(x(t)) \leq -\alpha_3(\alpha_2^{-1}(\rho_s)) + \left(L_x + \sum_{i=1}^{m} L_{\bar{u}_i}\bar{u}_i^{\max} \right) M\Delta + L_w\theta \tag{6.24}$$

When Eq. 6.10 is satisfied, there exists $\varepsilon_w > 0$ *such that the following inequality holds for* $S(x(t_k)) > S_{TH}$*:*

$$\dot{V}(x(t)) \leq -\varepsilon_w/\Delta \quad \forall\, t \in [t_k, t_{k+1}) \tag{6.25}$$

By integrating the bound of Eq. 6.25 on $t \in [t_k, t_{k+1})$*, we obtain that:*

$$V(x(t_{k+1})) \leq V(x(t_k)) - \varepsilon_w \tag{6.26a}$$

$$V(x(t)) \leq V(x(t_k)),\ \ \forall\, t \in [t_k, t_{k+1}) \tag{6.26b}$$

whenever $S(x(t_k)) > S_{TH}$ and the m Safeness Index-S-DLEMPC's are feasible. When Safeness Index-S-DLEMPC 1 has no feasible solution and $x(t_0) \in \Omega_\rho$, then $\overline{h}(x(t_k))$ is applied for $t \in [t_k, t_{k+1})$, which will decrease the value of the Lyapunov function between t_k and t_{k+1} according to Proposition 6.1. Therefore, regardless of whether $\overline{u}_i^*(t_k|t_k)$, $i = 1, \ldots, m$, or $\overline{h}(x(t_k))$ is implemented throughout a given sampling period when $S(x(t_k)) > S_{TH}$, $V(x(t_{k+1})) < V(x(t_k))$ and the sequence of control actions implemented until $S(x(t_k)) \leq S_{TH}$ will thus drive the closed-loop state into Lyapunov level sets with a smaller upper bound on the Lyapunov function. This will eventually drive the state into the safety zone, because the control actions will drive the state toward $\Omega_{\rho_{\min}}$ throughout every sampling period and thus into $\Omega_{\rho_{\min}}$ if $S(x(t_k))$ is greater than S_{TH} at every sampling time until $x(t_k) \in \Omega_{\rho_{\min}}$ (the state is within the safety zone after it is within $\Omega_{\rho_{\min}}$ from Eq. 6.19, regardless of the shape of the safety zone).

To prove that $x(t) \in \Omega_\rho$, $\forall\, t \in [t_0, \infty)$, when $x(t_0) \in \Omega_\rho$ for a process operated under the Safeness Index-S-DLEMPC implementation strategy, we begin by demonstrating that if $x(t_k) \in \Omega_\rho$, then $x(t) \in \Omega_\rho$, $\forall\, t \in [t_k, t_{k+1})$, both in the case that a feasible solution of the Safeness Index-S-DLEMPC design is applied to the process and in the case that $\overline{h}(x(t_k))$ is instead applied for $t \in [t_k, t_{k+1})$. When Safeness Index-S-DLEMPC 1 is feasible and $x(t_k) \in \Omega_{\rho_e}$ such that the constraint of Eq. 6.8g is applied and satisfied by the solution of Safeness Index-S-DLEMPC m under the implemented control actions $\overline{u}_i^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $i = 1, \ldots, m$, then $\tilde{x}^m(t) \in \Omega_{\rho_e}$ for $t \in [t_k, t_{k+1})$. From Propositions 6.2 and 6.3, and considering that the maximum value of $t - t_k$ for $t \in [t_k, t_{k+1})$ is Δ, we have that

$$V(x(t)) \leq V(\tilde{x}^m(t)) + f_V(f_W(\Delta)) \tag{6.27}$$

for $t \in [t_k, t_{k+1})$. Since $V(\tilde{x}^m(t)) \leq \rho_e$ for $t \in [t_k, t_{k+1})$ and Eq. 6.18 holds, we conclude that $x(t) \in \Omega_\rho$ for $t \in [t_k, t_{k+1})$. If $x(t_k) \in \Omega_\rho / \Omega_{\rho_e}$ (or $S(x(t_k)) > S_{TH}$), then Eq. 6.8i is active and Eqs. 6.26a-6.26b hold, preventing the closed-loop state from leaving Ω_ρ in a sampling period. When Safeness Index-S-DLEMPC 1 is not feasible, then $\overline{h}(x(t_k))$ will be applied for $t \in [t_k, t_{k+1})$, in which case Proposition 6.1 holds. A similar series of steps to those performed in Eqs. 6.20-6.26 can be performed when Proposition 6.1 holds, with the result that Eqs. 6.26a-6.26b hold when

Proposition 6.1 holds and therefore $x(t) \in \Omega_\rho$ for $t \in [t_k, t_{k+1})$. Since throughout each sampling period, a feasible solution to the m Safeness Index-S-DLEMPC's or $\overline{h}(x(t_k))$ maintains the closed-loop state within Ω_ρ, the sequence of control actions generated throughout time by applying either the Safeness Index-S-DLEMPC m solution or $\overline{h}(x(t_k))$ at each sampling time according to the Safeness Index-S-DLEMPC implementation strategy maintains the closed-loop state in Ω_ρ.

Finally, the closed-loop state under the Safeness Index-S-DLEMPC implementation strategy is ultimately bounded in $\Omega_{\rho_{\min}}$ when $t_k > t_s$ because when $t_k > t_s$, either a feasible solution to the m Safeness Index-S-DLEMPC's that had Eq. 6.8i applied is implemented for the process, or $\overline{h}(x(t_k))$ is implemented. In both cases, Eqs. 6.26a-6.26b hold and the Lyapunov function value decreases until the closed-loop state enters $\Omega_{\rho_{\min}}$ in finite time. After it enters $\Omega_{\rho_{\min}}$, it cannot come out due to the definition of $\Omega_{\rho_{\min}}$ in Eq. 6.11.

6.4.3 Safeness Index-based Iterative DLEMPC

In this section, we develop an iterative Safeness Index-based DLEMPC paradigm (Safeness Index-I-DLEMPC). In the iterative control design, each of the m controllers calculates a control action simultaneously. The j^{th} controller solves for $\overline{u}_j^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $j = 1, \ldots, m$, and assumes that the control actions for which it does not solve ($\overline{u}_z$, $z \in \{1, \ldots, m\}$, $z \neq j$) are set to $\overline{h}_z(\tilde{x}(t_q))$, $\forall\, t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$. After the solution for each controller is obtained, either this solution is applied to the process or is provided to (exchanged with) the other $m-1$ Safeness Index-I-DLEMPC's and each of the m controllers is then re-solved assuming that the control actions for which it does not solve are set to the values $\overline{u}_z^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $z \in \{1, \ldots, m\}$, $z \neq j$, that have just been exchanged. Each re-solution of all m optimization problems is called an iteration. The number of iterations of the Safeness Index-I-DLEMPC is an integer $c \in [1, \infty)$, where $c = 1$ corresponds to the case that the m controllers have not yet exchanged solutions. The termination condition for the iterations of the Safeness Index-I-DLEMPC design can be chosen in various ways; for example, a fixed number of iterations may be selected after which the solution of all m controllers is implemented on the process at t_k and the optimization problems no longer

exchange solutions. Another consideration to prevent further iterations at t_k is to terminate the optimization problem when the value of the objective function evaluated using the predicted nominal process state trajectories when $\overline{u}_i(t) = \overline{u}_i^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $i = 1, \ldots, m$, at iteration c shows no improvement compared to iteration $c-1$ or improves by no more than a tolerance ε. However, even with a termination condition based on the objective function, there is no guarantee that the economic performance of a nonlinear process under the Safeness Index-I-DLEMPC design will be comparable to that of the process under the centralized Safeness Index-based LEMPC since the manipulated inputs in the Safeness Index-I-DLEMPC are calculated by different controllers. The block diagram in Figure 6.2 shows the Safeness Index-I-DLEMPC, where the solution to Safeness Index-I-DLEMPC j at time t_k at iteration c is denoted by $\overline{u}_{j,c}^*(t|t_k)$, $t \in [t_k, t_{k+N})$.

The formulation of the j^{th} Safeness Index-I-DLEMPC optimization problem is as follows:

$$\max_{\bar{u_j}\in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}^j(\tau), \bar{u_1}(\tau), \ldots, \bar{u_m}(\tau)) d\tau \tag{6.28a}$$

$$\text{s.t. } \dot{\tilde{x}}^j(t) = f(\tilde{x}^j(t)) + \sum_{i=1}^{m} g_i(\tilde{x}^j(t))\bar{u_i}(t) \tag{6.28b}$$

$$\bar{u_j}(t) \in U_j, \ \forall\, t \in [t_k, t_{k+N}) \tag{6.28c}$$

$$\bar{u_z}(t) = \bar{h_z}(\tilde{x}^j(t_{k+r})), z \in \{1, \ldots, m\}, \tag{6.28d}$$

$$z \neq j, \ \forall\, t \in [t_{k+r}, t_{k+r+1}),$$

$$r = 0, \ldots, N-1, \ c = 1$$

$$\bar{u_z}(t) = \bar{u}^*_{z,c-1}(t|t_k), \ z \in \{1, \ldots, m\}, \tag{6.28e}$$

$$z \neq j, \ t \in [t_k, t_{k+N}), \ c \geq 2$$

$$\tilde{x}^j(t_k) = x(t_k) \tag{6.28f}$$

$$V(\tilde{x}^j(t)) \leq \rho_e, \ \forall\, t \in [t_k, t_{k+N}) \tag{6.28g}$$

$$\text{if } x(t_k) \in \Omega_{\rho_e}$$

$$S(\tilde{x}^j(t)) \leq S_{TH}, \ \forall\, t \in [t_k, t_{k+N}) \tag{6.28h}$$

$$\text{if } S(x(t_k)) \leq S_{TH}$$

$$\frac{\partial V(x(t_k))}{\partial x} g_j(x(t_k))\bar{u_j}(t_k) \leq \frac{\partial V(x(t_k))}{\partial x} g_j(x(t_k))\bar{h}_j(x(t_k)), \tag{6.28i}$$

$$\text{if } x(t_k) \in \Omega_\rho / \Omega_{\rho_e} \text{ or } t_k > t_s \text{ or } S(x(t_k)) > S_{TH}$$

The notation of Eqs. 6.28a-6.28c and Eqs. 6.28f-6.28h follows that in Eq. 6.8. Eq. 6.28d is applied when $c = 1$ (i.e., no iteration has yet been performed at t_k) and assumes $\bar{u_z}(t)$ is $\bar{h_z}(x)$, $z \neq j$, implemented in sample-and-hold throughout the prediction horizon. Eq. 6.28e is applied if $c > 1$ and sets $\bar{u_z}(t)$, $z \in \{1, \ldots, m\}$, where $z \neq j$, to the optimal solutions obtained from all Safeness Index-I-DLEMPC's except the j^{th} at the prior iteration. Unlike the constraint of Eq. 6.8i, in which all inputs appear, the contractive constraint of Eq. 6.28i only constrains the decision

variable $\bar{u}_j(t_k)$.

To obtain a solution to the Safeness Index-I-DLEMPC design at t_k, all m Safeness Index-I-DLEMPC's must be feasible simultaneously. It may be more likely for all m controllers to be feasible at t_k when Eq. 6.28h is applied if each vector $\bar{u}_i$, $i = 1, \ldots, m$, contains control actions that have a significant impact on $S(x)$ and therefore may give each of the m distributed controllers more flexibility to satisfy Eq. 6.28h. For some processes, feasibility of the m Safeness Index-I-DLEMPC's for several iterations may improve process economic performance because the controllers can exchange solutions and re-solve Eq. 6.28 to attempt to improve process economic performance only if the solutions of all m controllers at the prior iteration are feasible. Unlike the computation time of the Safeness Index-S-DLEMPC, which is equal to the summation of the computation times of each of the m controllers, the computation time of the iterative control architecture (at one iteration) is equal to the maximum computation time among all m Safeness Index-I-DLEMPC's (the sum of the computation times of all iterations performed is the total computation time of the iterative architecture). This indicates that increasing the number of distributed controllers (i.e., increasing m) may improve the computation time compared to using a smaller m because it parallelizes the computations more significantly. As noted in the section "Safeness Index-based Sequential DLEMPC," constraints beyond those noted in Eq. 6.28 may be required to be satisfied by the process and may affect the input partitioning. Therefore, tradeoffs between feasibility, computation time, and economic performance may affect input partitioning for the Safeness Index-I-DLEMPC design.

The solutions of the m Safeness Index-I-DLEMPC's are calculated independently, with each controller assuming different values of $\bar{u}_z$, $z \in \{1, \ldots, m\}$ but $z \neq j$, than are used by the other controllers (e.g., Safeness Index-I-DLEMPC 1 assumes for $c = 1$ that $\bar{u}_1$ can be any piecewise-constant input trajectory that satisfies the constraints of Eq. 6.28, but assumes that $\bar{u}_2 = \bar{h}_2(\tilde{x}(t_q))$, $\forall\ t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$, whereas Safeness Index-I-DLEMPC 2 assumes that $\bar{u}_1 = \bar{h}_1(\tilde{x}(t_q))$, $\forall\ t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$, but that $\bar{u}_2$ can be any piecewise-constant input trajectory that satisfies the constraints of Eq. 6.28). Therefore, all m controllers may be feasible (i.e., Eqs. 6.28g-6.28h may be satisfied in Safeness Index-I-DLEMPC j by the nominal trajec-

tory of Eq. 6.1 under $\bar{u}_j^*(t|t_k)$, $t \in [t_k, t_{k+N})$, and the assumed control actions in Eqs. 6.28d-6.28e), but Eqs. 6.28g-6.28h may not be satisfied for the nominal system of Eq. 6.1 under the trajectories $\bar{u}_{1,c}^*, (t|t_k) \ldots, \bar{u}_{m,c}^*(t|t_k)$, $t \in [t_k, t_{k+N})$ (this trajectory is denoted by $\tilde{x}^{tot}$ in the following) returned by the set of m Safeness Index-I-DLEMPC's at iteration c since that was not a condition required for feasibility of any of the m Safeness Index-I-DLEMPC's. Nevertheless, iteration $c+1$ is not guaranteed to be feasible unless $\tilde{x}^{tot}$ meets the constraints of Eqs. 6.28g-6.28h. Therefore, satisfaction of those constraints by the control actions returned at iteration c should be checked before a new iteration is performed. If Eqs. 6.28g-6.28h are not satisfied by $\tilde{x}^{tot}$ and $c > 1$, the solution from iteration $c-1$ should be implemented (this implementation strategy ensures that the solution from iteration $c-1$ causes Eqs. 6.28g-6.28h to be met or iteration c would not have been performed). If Eqs. 6.28g-6.28h are not satisfied by $\tilde{x}^{tot}$ and $c = 1$, then $\bar{h}(x(t_k))$ should be implemented (the solution to the m Safeness Index-I-DLEMPC's should not be implemented because satisfaction of Eqs. 6.28g-6.28h by $\tilde{x}^{tot}$ is required for the closed-loop stability results in the next section). This gives the following implementation strategy of the Safeness Index-I-DLEMPC design:

1. At t_k, all m Safeness Index-I-DLEMPC's receive a measurement of the current state $x(t_k)$ from the sensors. Go to Step 2 ($c = 1$).

2. An attempt is made to solve all m Safeness Index-I-DLEMPC optimization problems. If $c = 1$, Safeness Index-I-DLEMPC j assumes $\bar{u}_z(t) = \bar{h}_z(\tilde{x}^j(t_{k+r}))$, $\forall\ t \in [t_{k+r}, t_{k+r+1})$, $z \in \{1, \ldots, m\}$ but $z \neq j$, $r = 0, \ldots, N-1$. If $c > 1$, Safeness Index-I-DLEMPC j assumes $\bar{u}_z(t) = \bar{u}_{z,c-1}^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $z \in \{1, \ldots, m\}$ but $z \neq j$. If all m Safeness Index-I-DLEMPC's are feasible, go to Step 3. Else, go to Step 4.

3. Evaluate whether $V(\tilde{x}^{tot}(t)) \leq \rho_e$ and $S(\tilde{x}^{tot}(t)) \leq S_{TH}$, $\forall\ t \in [t_k, t_{k+N})$. Also, evaluate whether the iteration termination conditions are met (e.g., the objective function evaluated for $\tilde{x}^{tot}$ and $\bar{u}_{i,c}^*(t|t_k)$, $i = 1, \ldots, m$, $t \in [t_k, t_{k+N})$ fails to improve between two iterations). If Eqs. 6.28g-6.28h are not satisfied by $\tilde{x}^{tot}$ or the iteration termination condition is met, go to Step 4. Else, any information required for evaluating the iteration termination condition

(e.g., the objective function value) is stored, and go to Step 5 ($c \leftarrow c+1$).

4. If $c > 1$, implement $[\bar{u}_1^*(t_k|t_k) \ \ldots \ \bar{u}_m^*(t_k|t_k)] = [\bar{u}_{1,c-1}^*(t_k|t_k) \ \ldots \ \bar{u}_{m,c-1}^*(t_k|t_k)]$. Else, implement $[\bar{u}_1^*(t_k|t_k) \ \ldots \ \bar{u}_m^*(t_k|t_k)] = [\bar{h}_1(x(t_k)) \ \ldots \ \bar{h}_m(x(t_k))]$. Go to Step 6.

5. Safeness Index-I-DLEMPC j receives the optimal solutions $\bar{u}_{z,c-1}^*(t|t_k)$, $z = 1,\ldots,m$, $z \neq j$, $t \in [t_k, t_{k+N})$, for $j = 1,\ldots,m$. Go to Step 2.

6. When a new state measurement is received at t_{k+1}, go to Step 1 ($k \leftarrow k+1$).

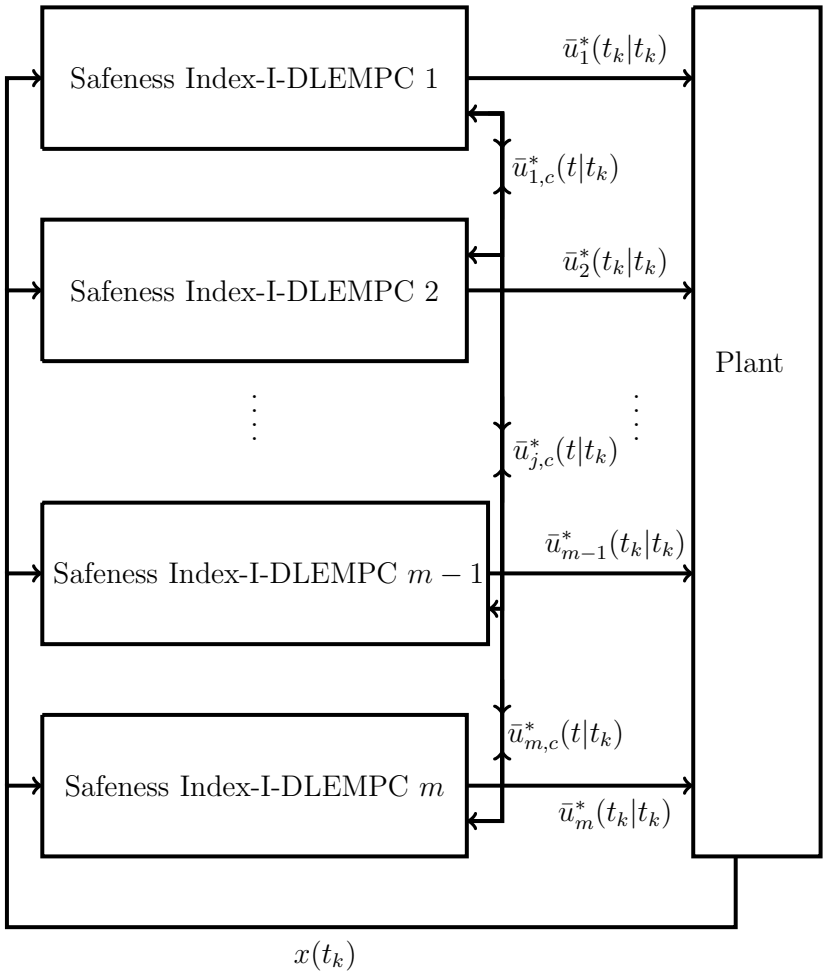

Figure 6.2: Block diagram of the Safeness Index-I-DLEMPC scheme.

6.4.4 Feasibility and Closed-Loop Stability Analysis for the Safeness Index-I-DLEMPC Implementation Strategy

The following theorem provides sufficient conditions under which the implementation strategy of the Safeness Index-I-DLEMPC is guaranteed to maintain closed-loop stability of a nonlinear process.

Theorem 6.2 *Consider the system of Eq. 6.1 in closed-loop under the implementation strategy (Steps 1-6) of the Safeness Index-I-DLEMPC based on a controller* $\overline{h}(x)$ *that satisfies the conditions of Eq. 6.2. Let* $\varepsilon_w > 0$, $\Delta > 0$, $\rho > \rho_e > \rho_s > 0$ *satisfy Eqs. 6.18 and 6.10. If* $x(t_0) \in \Omega_\rho$, $\rho_{\min} \leq \rho_e$ *and* $N \geq 1$ *where* $\rho_{\min}$ *is defined as in Eq. 6.11 and where the compact set* $\Omega_{\rho_{\min}}$ *satisfies Eq. 6.19, then the closed-loop state* $x(t)$ *of Eq. 6.1 is guaranteed to enter the safety zone in finite time when* $x(t_0) \in \Omega_\rho$, *to be bounded within* Ω_ρ *at all times, and to be ultimately bounded in* $\Omega_{\rho_{\min}}$.

Proof 6.2 *The proof consists of two parts. In Part 1, we demonstrate that the inputs applied to the process at every sampling time have characterizable properties. In Part 2, we demonstrate that this sequence of characterizable inputs guarantees the results of Theorem 6.2.*

Part 1. At each sampling time, according to the implementation strategy of the Safeness Index-I-DLEMPC, either $\overline{h}(x(t_k))$ *is implemented on the process, or a feasible solution to all m Safeness Index-I-DLEMPC's (i.e., a solution satisfying Eqs. 6.28b-6.28i in Safeness Index-I-DLEMPC i,* $\forall\ i = 1, \ldots, m$*) is implemented that ensures* $V(\tilde{x}^{tot}) \leq \rho_e$ *and* $S(\tilde{x}^{tot}) \leq S_{TH}$ *from Step 3 of the implementation strategy (feasibility of Safeness Index-I-DLEMPC's 1 to m ensures that each implemented input* $\overline{u}_i^*(t|t_k)$, $t \in [t_k, t_{k+1})$, $i = 1, \ldots, m$, *satisfies Eqs. 6.28c and 6.28i because satisfaction of these constraints depends only on the value of* $\overline{u}_j^*(t|t_k)$ *calculated by the controller and is not affected by the values of* $u_z^*(t|t_k)$, $t \in [t_k, t_{k+N})$, $z \in \{1, \ldots, m\}$, $z \neq j$*). When* $c = 1$, *there is no guarantee that a feasible solution to Eq. 6.28 exists in any of the m Safeness Index-I-DLEMPC's when Eq. 6.28h is applied (however, a feasible solution* $\overline{u}_{i,1}^*(t|t_k) = \overline{h}_i(\tilde{x}(t_q))$, $\forall\ t \in [t_q, t_{q+1})$, $q = k, \ldots, k+N-1$, *is guaranteed for Safeness Index-I-DLEMPC i,* $i = 1, \ldots, m$, *when Eq. 6.28h is not applied because this manipulated input trajectory satisfies Eq. 6.28c from Eq. 6.2, it sat-*

isfies Eq. 6.28g when combined with the manipulated input trajectories of Eq. 6.28d by Eq. 6.12 when $\rho_{\min} \leq \rho_e$, and it trivially satisfies Eq. 6.28i). When $c > 1$, each iteration performed is guaranteed to have a feasible solution. To show this, it is noted that if iteration c is attempted, then $\overline{u}^*_{i,c-1}(t|t_k)$, $t \in [t_k, t_{k+N})$, $i = 1, \ldots, m$, met Eqs. 6.28c and 6.28i from feasibility of those constraints at iteration $c-1$ and ensured that Eqs. 6.28g-6.28h were satisfied by the nominal solution of Eq. 6.1 under $\overline{u}^*_{i,c-1}(t|t_k)$, $t \in [t_k, t_{k+N})$, $i = 1, \ldots, m$, by Step 3 of the Safeness Index-I-DLEMPC implementation strategy. At iteration c, Safeness Index-I-DLEMPC j sets $\overline{u}^*_{z,c}(t|t_k) = \overline{u}^*_{z,c-1}(t|t_k)$, $t \in [t_k, t_{k+N})$, $z \in \{1, \ldots, m\}$, $z \neq j$, by Eq. 6.28e (the input trajectory for the prior iteration except for $\overline{u}^*_{j,c-1}(t|t_k)$). Therefore, $\overline{u}^*_{j,c}(t|t_k) = \overline{u}^*_{j,c-1}(t|t_k)$, $t \in [t_k, t_{k+N})$, is a feasible solution to Safeness Index-I-DLEMPC j because it is guaranteed to satisfy all constraints in Eq. 6.28 at iteration c since it satisfied them at iteration $c-1$ (even when the constraint of Eq. 6.28h is applied). When any of the m Safeness Index-I-DLEMPC's is infeasible for $c = 1$, $\overline{h}(x(t_k))$ is implemented, and Proposition 6.1 holds. Thus, whether a feasible solution to the Safeness Index-I-DLEMPC's is implemented or $\overline{h}(x(t_k))$, the implemented solution is characterizable and closed-loop stability of a nonlinear system under such control actions can be analyzed.

Part 2. We will now prove the three results of Theorem 6.2. First, we prove that the Safeness Index-I-DLEMPC implementation strategy guarantees that the closed-loop state will enter the safety zone in finite time whenever $x(t_k) \in \Omega_\rho$ but $S(x(t_k)) > S_{TH}$. At each sampling time that $S(x(t_k)) > S_{TH}$ and a feasible solution to the m Safeness Index-I-DLEMPC's meeting the conditions checked in Step 3 of the Safeness Index-I-DLEMPC implementation strategy is implemented on the process, the constraint of Eq. 6.28i is applied in each of the m Safeness Index-I-DLEMPC's. Summing these constraints gives Eq. 6.20a, and the results developed through Eqs. 6.20-6.26 in the proof of Theorem 6.1 hold, showing that $V(x(t_{k+1})) < V(x(t_k))$. Alternatively, if $\overline{h}(x(t_k))$ is applied at t_k when $S(x(t_k)) > S_{TH}$, then by Proposition 6.1, $V(x(t_{k+1})) < V(x(t_k))$. This indicates that at each sampling time that $S(x(t_k)) > S_{TH}$, the implementation strategy of the Safeness Index-I-DLEMPC drives $x(t)$ from a Lyapunov level set to one with a lower upper bound on the Lyapunov function. The state will either enter the safety zone before it enters $\Omega_{\rho_{\min}}$ or will be driven to $\Omega_{\rho_{\min}}$

(contained within the safety zone from Eq. 6.19) in finite time.

We next prove that the closed-loop state remains bounded in Ω_ρ at all times under the Safeness Index-I-DLEMPC implementation strategy. When a feasible solution to the Safeness Index-I-DLEMPC is implemented on the process, this solution satisfies the constraint of Eq. 6.28g for $\tilde{x}^{tot}$ and/or the constraint of Eq. 6.28i. When the constraint of Eq. 6.28i is applied (regardless of whether the constraint of Eq. 6.28g is simultaneously applied), the analysis from the prior paragraph indicates that Eq. 6.26b holds and therefore, $V(x(t)) \leq V(x(t_k))$, $\forall\, t \in [t_k, t_{k+1})$, so that the state cannot leave Ω_ρ within Δ if $x(t_k) \in \Omega_\rho$. If Eq. 6.28g is applied but Eq. 6.28i is not (i.e., $x(t_k) \in \Omega_{\rho_e}$, $t_k < t_s$, and $S(x(t_k)) \leq S_{TH}$), then utilizing Propositions 6.2 and 6.3, Eq. 6.18, and Eq. 6.28g, we conclude that Eq. 6.27 holds and that $x(t) \in \Omega_\rho$, $\forall\, t \in [t_k, t_{k+1})$, if $x(t_k) \in \Omega_{\rho_e}$. If $\bar{h}(x(t_k))$ is implemented on the process and Eq. 6.10 holds, then Eqs. 6.20-6.26 hold and Eq. 6.26b shows that $x(t)$ cannot leave Ω_ρ in Δ if $x(t_k) \in \Omega_\rho$. Therefore, under the implementation strategy of the Safeness Index-I-DLEMPC, the implemented control action at t_k ensures that $x(t) \in \Omega_\rho$, $\forall\, t \in [t_k, t_{k+1})$, whenever $x(t_k) \in \Omega_\rho$ and therefore, $x(t) \in \Omega_\rho$ throughout the length of operation if $x(t_0) \in \Omega_\rho$.

Finally, we prove that the closed-loop state is ultimately bounded in $\Omega_{\rho_{\min}}$ when $t_k > t_s$. In this case, either Eq. 6.28i holds (if a feasible solution to the Safeness Index-I-DLEMPC is implemented) or $\bar{h}(x(t_k))$ is implemented. In both cases from the analysis above, $V(x(t_{k+1})) < V(x(t_k))$ for $x(t_k) \in \Omega_\rho / \Omega_{\rho_s}$. Once $x(t_k) \in \Omega_{\rho_s}$, then by definition of $\Omega_{\rho_{\min}}$, the closed-loop state will not leave $\Omega_{\rho_{\min}}$.

6.5 Application to a Chemical Process Example

The two proposed distributed control schemes and the centralized Safeness Index-based LEMPC are compared through an ethylene oxidation example. Three oxidation reactions[12] convert ethylene to ethylene oxide in a continuous stirred tank reactor (CSTR) with a cooling/heating jacket for

which the dimensionless mass and energy balances are:[77]

$$\frac{dx_1}{dt} = u_1(1 - x_1x_4) \tag{6.29a}$$

$$\frac{dx_2}{dt} = u_1(u_2 - x_2x_4) - A_1e^{\frac{\gamma_1}{x_4}}(x_2x_4)^{0.5} - A_2e^{\frac{\gamma_2}{x_4}}(x_2x_4)^{0.25} \tag{6.29b}$$

$$\frac{dx_3}{dt} = -u_1x_3x_4 + A_1e^{\frac{\gamma_1}{x_4}}(x_2x_4)^{0.5} - A_3e^{\frac{\gamma_3}{x_4}}(x_3x_4)^{0.5} \tag{6.29c}$$

$$\frac{dx_4}{dt} = \frac{u_1}{x_1}(1 - x_4) + \frac{B_1}{x_1}e^{\frac{\gamma_1}{x_4}}(x_2x_4)^{0.5} \tag{6.29d}$$
$$+ \frac{B_2}{x_1}e^{\frac{\gamma_2}{x_4}}(x_2x_4)^{0.25} + \frac{B_3}{x_1}e^{\frac{\gamma_3}{x_4}}(x_3x_4)^{0.5} - \frac{B_4}{x_1}(x_4 - u_3)$$

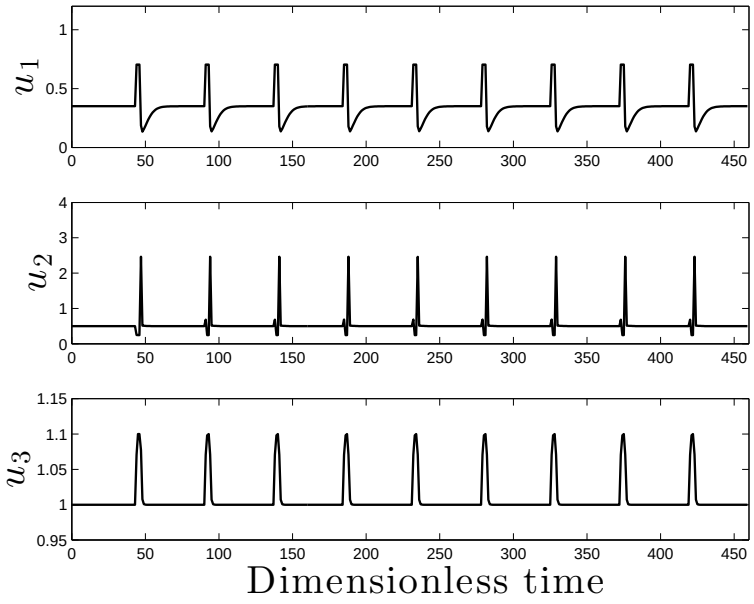

Figure 6.3: The manipulated input profile of the catalytic reactor under the Safeness Index-I-DLEMPC.

Because u_2 only appears in the u_1u_2 term of $\dot{x}_2$, we can define $u_4 = u_1u_2$ so that the form of Eq. 6.29 resembles that of Eq. 6.1. The manipulated inputs u_1, u_2 and u_3 are the dimensionless feed volumetric flow rate, the concentration of ethylene in the feed, and the coolant temperature, respectively. The state variables x_1, x_2, x_3, and x_4 represent the dimensionless gas density, ethylene concentration, ethylene oxide concentration, and the reactor temperature, respectively. The values of the parameters in Eq. 6.29 can be found in.[9] The manipulated inputs are constrained by

physical actuator limitations as follows: $0.0704 \leq u_1 \leq 0.7042$, $0.2465 \leq u_2 \leq 2.4648$, $0.6 \leq u_3 \leq 1.1$. The process of Eq. 6.29 is operated around the asymptotically stable steady-state $[x_{1s}\ x_{2s}\ x_{3s}\ x_{4s}] = [0.998\ 0.424\ 0.032\ 1.002]$ that corresponds to the manipulated input values of $[u_{1s}\ u_{2s}\ u_{3s}] = [0.35\ 0.5\ 1.0]$. The control objective is to maximize the average yield of ethylene oxide, which is computed over a time period from t_0 to ct_f by:

$$Y(t_e) = \frac{\int_{t_0}^{ct_f} u_1(\tau)x_3(\tau)x_4(\tau)\ d\tau}{\int_{t_0}^{ct_f} u_1(\tau)u_2(\tau)\ d\tau} \tag{6.30}$$

where ct_f is an integer multiple ($c = 10$) of the length of the operating period $t_f = 47$. For practical reasons, the average amount of material that may be fed to the reactor over each operating period t_f is fixed as follows:

$$\frac{1}{t_f}\int_{(j-1)t_f}^{jt_f} u_1(\tau)u_2(\tau)\ d\tau = u_{1s}u_{2s} = 0.175 \tag{6.31}$$

where $j = 1, 2, \ldots, 10$. Since the material constraint of Eq. 6.31 fixes the denominator of Eq. 6.30, the centralized and distributed Safeness Index-based LEMPC schemes will only maximize the following stage cost:

$$L_e(x,u) = u_1x_3x_4. \tag{6.32}$$

A characterization of the closed-loop stability region Ω_ρ is developed using a Lyapunov-based controller $h^T(x) = [h_1(x)\ h_2(x)\ h_3(x)]$ where each component is a PI controller with the form $h_a(x) = K_{P_a}(x_a - x_{as}) + \frac{1}{\tau_a}\int_0^t (x_a - x_{as})dt$, $a = 1, 2, 3$, where $K_{P_1} = 3.0$, $K_{P_2} = 0.105$, $K_{P_3} = 0.1$, $\tau_1 = 0.00001$, $\tau_2 = 0.0002081$, and $\tau_3 = 0.005$. The quadratic Lyapunov function $V(x) = (x - x_s)^T P(x - x_s)$ where the positive definite matrix P is P=diag[1 1 1 1] was used to estimate the stability region Ω_ρ where $\rho = 2.1$. The Lyapunov-based constraints of the distributed and centralized Safeness Index-based LEMPC's were Eqs. 6.7e, 6.8g, and 6.28g; in this example, the contractive constraints of Eqs. 6.7g, 6.8i, and 6.28i were not applied because no closed-loop stability or safety issues were encountered during the simulation, and therefore ρ_e was set to ρ in Eqs. 6.7e, 6.8g, and 6.28g. The Explicit Euler numerical integration method with an integration

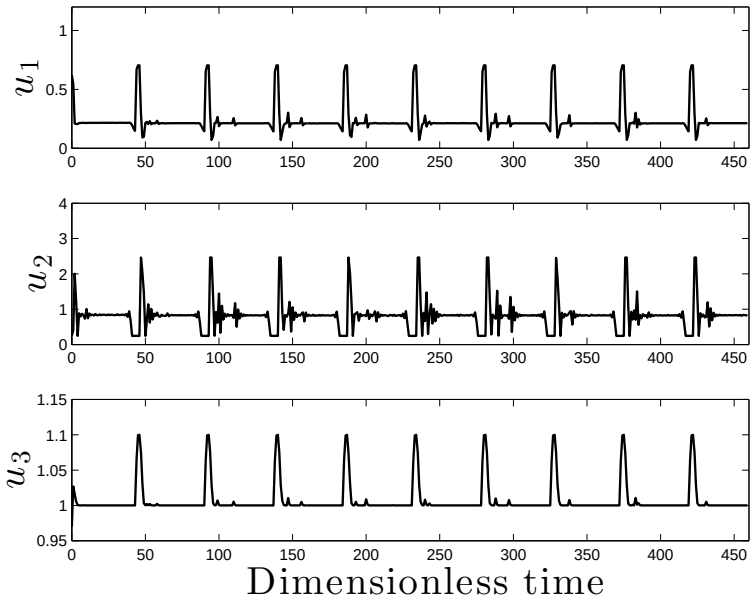

Figure 6.4: The manipulated input profile of the catalytic reactor under the Safeness Index-S-DLEMPC.

step size of $h_I = 10^{-5}$ was used to simulate the process of Eq. 6.29 and an integration step size of $h_O = 0.005$ was used to integrate the model of Eq. 6.29 within the optimization problems. The interior-point solver Ipopt[90] was used to solve all LEMPC optimization problems. The LEMPC's are implemented with a shrinking prediction horizon so that at $t_k = (j-1)t_f$, $j = 1,\ldots,10$, where the operating window $t_f = 47$, the prediction horizon N is set to t_f/Δ for $\Delta = 1$, but N is then decreased by one at each subsequent sampling time between $(j-1)t_f$ and jt_f. No feasibility issues were encountered for any of the optimization problems performed. However, after every iteration of the iterative Safeness Index-based LEMPC, the conditions $V(\tilde{x}^{tot}) \leq \rho$ and $S(\tilde{x}^{tot}) \leq S_{TH}$ and the iteration termination condition (terminate the optimization problem when the integral of the stage cost of Eq. 6.32 over the prediction horizon calculated using the solutions to the m Safeness Index-I-DLEMPC's at iteration c is no better than the value at iteration $c-1$) were checked. When these conditions indicated that no second iteration should be performed, $h(x(t_k))$ was applied to the process. The number of iterations performed at a given sampling time using this strategy was at most 4.

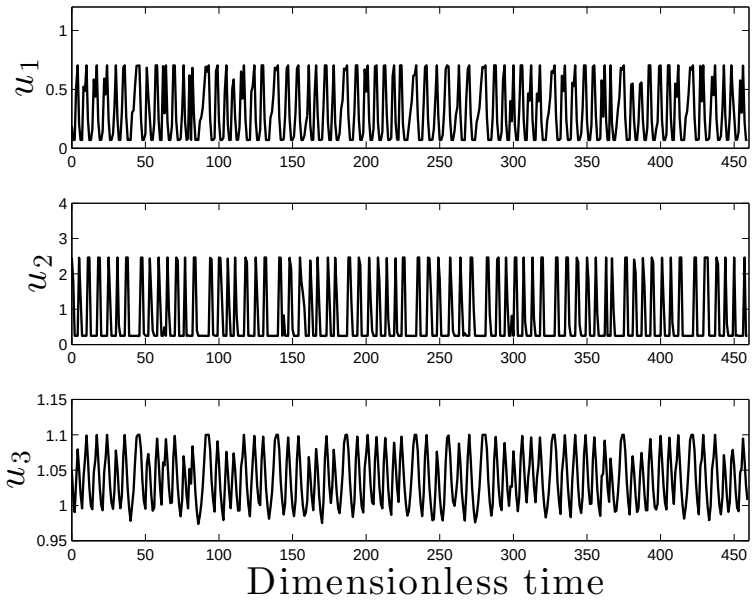

Figure 6.5: The manipulated input profile of the catalytic reactor under the centralized Safeness Index-based LEMPC.

The Safeness Index for this example was designed to incorporate both the concentration of ethylene oxide (since it is a flammable, reactive, and toxic gas) and the temperature in the reactor (which we considered to be a quantity that we want to bound) as follows:

$$S(x) = \frac{ax_3 + bx_4}{\max\{ax_3 + bx_4 : x_3, x_4 \in S_s\}} \tag{6.33}$$

where a and b are weighting constants, and S_s is a set utilized in analyzing expected values of the Safeness Index for determining a threshold for $S(x)$. Specifically, based on prior works in which the process of Eq. 6.29 was controlled using EMPC (e.g.,[9]), the following estimated ranges in which the values of the process states were expected to remain when the process is operated under EMPC were developed: $x_1 \in [0.98, 1]$, $x_2 \in [0, 2]$, $x_3 \in [0, 0.25]$, $x_4 = [0.7, 1.03]$. The set of all x_1, x_2, x_3, and x_4 for which those states are in their respective bounds defines S_s. Based on these ranges, a and b are set to 5 and 2 so that when x_3 and x_4 take their maximum values in S_s, the terms ax_3 and bx_4 in $S(x)$ are on the same order of magnitude. To determine an appropriate value of S_{TH},

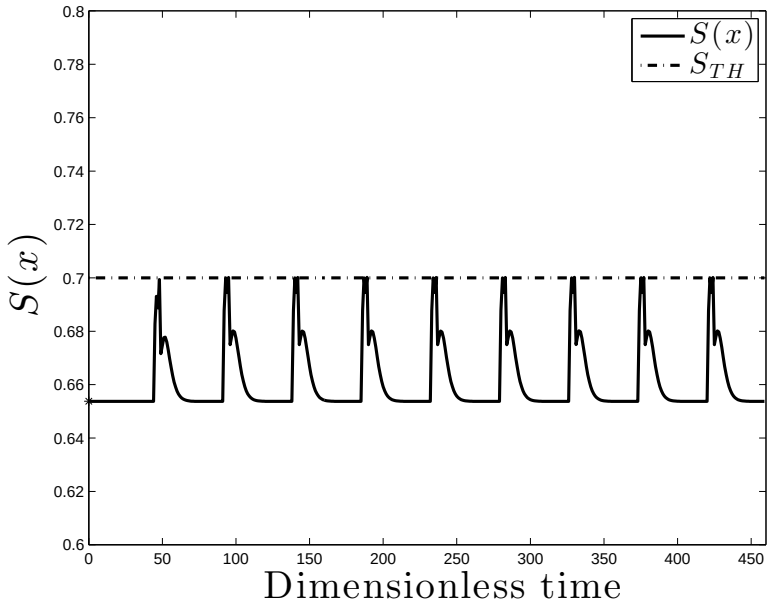

Figure 6.6: The value of the Safeness Index function $S(x)$ under the Safeness Index-I-DLEMPC.

the value of $S(x)$ was analyzed at many points throughout S_s through numerical simulations, and the maximum value observed was $S(x) = 3.31$, which is used as the denominator in Eq. 6.33 (i.e., $\max\{ax_3 + bx_4 : x_3, x_4 \in S_s\}$ was defined to be 3.31 in Eq. 6.33).

The threshold S_{TH} was set to 0.7 to attempt to prevent the value of x_3 from exceeding about 75% of the maximum value of 0.25 within the expected region of operation defined by S_s, and to attempt to prevent the value of x_4 from getting more than about 15% larger within S_s than the feed temperature which was used as the reference temperature for making x_4 dimensionless in.[77]

For both distributed Safeness Index-based LEMPC's, the partitioning of the manipulated inputs was based on the constraint of Eq. 6.31 (i.e., because the constraint is enforced on the product of u_1 and u_2, the inputs u_1 and u_2 were solved by one distributed controller and u_3 was solved by another). The dynamic model of Eq. 6.29 under all control strategies was initiated from the steady-state point $x(t_0)^T = [0.998\ 0.424\ 0.032\ 1.002]$ where the value of the Safeness Index $S(x)$ is equal to 0.65 which is less than threshold value $S_{TH} = 0.7$ (this satisfies the assumption that the steady-state is inside the safety zone). Figures 6.3-6.5 represent the manipulated input profiles under the Safeness Index-I-DLEMPC, the Safeness Index-S-DLEMPC, and the centralized Safeness Index-

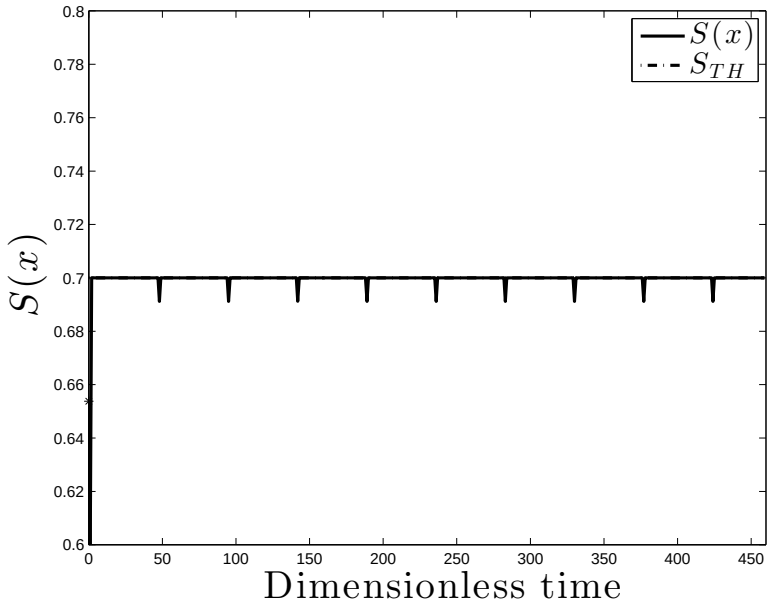

Figure 6.7: The value of the Safeness Index function $S(x)$ under the Safeness Index-S-DLEMPC. $S(x)$ overlays S_{TH} in the figure throughout much of the time of operation.

Table 6.1: The average yield and computation time under the distributed and centralized Safeness Index-based LEMPC strategies.

Strategy	Yield (%)	Computation Time (s)
Safeness Index-S-DLEMPC	7.72	7.37
Safeness Index-I-DLEMPC	6.60	6.167
Safeness Index-C-LEMPC	8	10.1

based LEMPC, respectively. From these figures, the manipulated inputs under all control strategies exhibit periodic operation so that the ethylene is distributed in a non-uniform fashion with respect to time to maximize the yield of ethylene oxide. In addition, the material constraint of Eq. 6.31 was met under all three control strategies over each operating window.

Figures 6.6-6.8 show the Safeness Index value under the distributed and centralized control strategies. From these figures, both the distributed and centralized Safeness Index-based LEMPC's were able to maintain the closed-loop state within the safety zone during the time of operation. The value of $S(x)$ evolves periodically due to the periodic nature of the optimal solution of the input profile. Table 6.1 shows the average computation time and yield under the two distributed

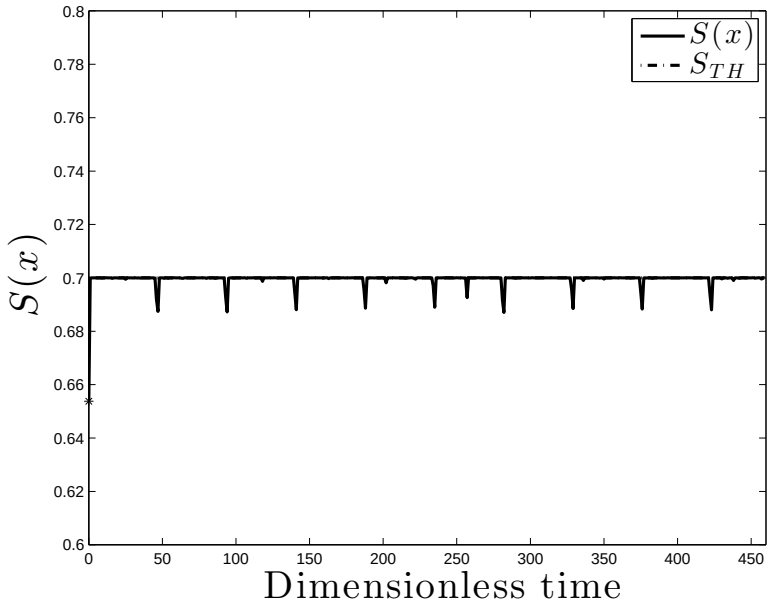

Figure 6.8: The value of the Safeness Index function $S(x)$ under the centralized Safeness Index-based LEMPC. $S(x)$ overlays S_{TH} in the figure throughout much of the time of operation.

Safeness Index-based LEMPC's and under the centralized Safeness Index-based LEMPC (denoted by Safeness Index-C-LEMPC in the table). From the table, the centralized Safeness Index-based LEMPC requires almost 40% more computation time than the Safeness Index-S-DLEMPC and requires over 60% more computation time than the Safeness Index-I-DLEMPC. The yield of the Safeness Index-S-DLEMPC is about 15% greater than that of the Safeness Index-I-DLEMPC and is close to that of the centralized design (the yield for the centralized design is only about 4% greater), but it requires 16% more computation time than the Safeness Index-I-DLEMPC. Due to the conditions on $V(\tilde{x}^{tot})$ and $S(\tilde{x}^{tot})$ and the iteration termination condition that must be met at the end of each iteration for the Safeness Index-I-DLEMPC, the iterations for this control design frequently terminated after the second iteration so that the $c = 1$ solution was applied. The lack of communication between the controllers when the $c = 1$ solution is applied, or the application of $h(x(t_k))$ instead of an optimal solution to the optimization problem when the $c = 1$ solution does not meet the termination criteria, may contribute to the lower economic performance of the iterative control design for this example than the sequential design. However, all control designs

were successful at keeping $S(x) \leq S_{TH}$ at all times.

6.6 Conclusion

In this chapter, sequential and iterative DLEMPC designs were developed with constraints based on a Safeness Index. Implementation strategies were developed for each that guarantee closed-loop stability of a nonlinear process. A chemical process example demonstrated that the computation time may be lower for the DLEMPC designs than for a centralized LEMPC design with Safeness Index-based constraints.

Chapter 7

Conclusions

Due to the increasing importance of the safety and economic objectives of process operation, this dissertation developed different methods for integrating process operational safety and process economics with advanced process control system design. In addition, we developed for the first time a metric termed the Safeness Index that can quantify the safeness of each point in state-space, and then developed an EMPC scheme that can utilize a threshold on this index to maintain the closed-loop state within a safety zone. To reduce the computation time issues introduced by the centralized safety-based EMPC designs, various distributed EMPC paradigms were developed with guaranteed closed-loop stability and recursive feasibility.

Specifically, in Chapter 2, an implementation strategy was presented for systems where a safe level set of operation is evaluated on-line within which the closed-loop state can vary throughout time. Various Lyapunov-based EMPC schemes that can utilize this safety level set were proposed. The first safety-LEMPC utilizes a constraint based on a Lyapunov-based controller to drive the state into a safe level set; however, the rate at which the state approaches the safety level set under this scheme may be long. To drive the process states into the safety level set by a pre-specified time, an LEMPC design that uses a sufficiently long prediction horizon and a region constraint was developed. Due to the computation time difficulties that can be introduced by such a scheme, two LEMPC formulations with tuning parameters that can be used to modify the rate of

transition of the closed-loop state to the safety region without the need for a long prediction horizon to ensure feasibility/stability were proposed. The first safety-based LEMPC formulation utilizes slack variables to adjust the Lyapunov function bound, and the second one decreases the upper bound on the Lyapunov function dynamically. Closed-loop stability in the sense of boundedness of the closed-loop state and recursive feasibility was proved under each scheme.

Chapter 3 developed two LMPC schemes with safety-based constraints that can integrate feedback control and process functional safety. The motivation for the proposed safety-LMPC design is to drive the closed-loop state to a safe region of operation at a desired rate, which cannot easily be accomplished by tuning the weighting matrices in the quadratic objective function. These two safety-based LMPC paradigms ensure process safety by varying the upper bound on the level set of the Lyapunov function to seek to improve the rate of approach of the process state to the safety region. In addition, these two schemes can also be modified to shift the region of operation from a level set around one steady-state to a level set around another. Recursive feasibility and closed-loop stability of a class of nonlinear systems under one of the safety-LMPC formulations in the presence of uncertainty was proved for a sufficiently small sampling period.

Since the aforementioned safety-based EMPC designs were implemented with a centralized control paradigm, this dissertation developed various distributed safety-based EMPC formulations for a class of nonlinear processes to reduce the computation time issues that can be introduced by the centralized EMPC. Specifically, in Chapter 4, sequential and iterative Safety-DLEMPC schemes were developed as alternative control techniques to the centralized Safety-LEMPC. The motivation for developing these two distributed safety-based LEMPC schemes is to achieve less on-line computation time while attaining similar closed-loop performance and safety constraints satisfaction with respect to the centralized one. An implementation strategy and mathematical formulation for the Safety-Sequential-DLEMPC design and the Safety-Iterative-DLEMPC design were developed. Recursive feasibility and closed-loop stability of a class of nonlinear systems under the Safety-S-DLEMPC and Safety-I-DLEMPC formulations in the presence of uncertainty were proved for a sufficiently small sampling period. Utilizing a chemical process example, the

proposed iterative and sequential Safety-DLEMPC strategies were able to yield comparable closed-loop performance while significantly decreasing the on-line computation time compared to that required to solve the centralized Safety-LEMPC.

Subsequently, in Chapter 5, a new metric termed Safeness Index that can coordinate, for the first time, the control and safety systems within a chemical process plant was developed. A systematic approach for defining the functional form of the Safeness Index was given, and a methodology of choosing the threshold of the Safeness Index was presented. To efficiently utilize this Safeness Index within a control system, an LEMPC scheme with a hard Safeness Index-based constraint was proposed to integrate feedback control, process safety and process economics within a unified framework. Since the safety zone defined by this constraint is not necessary forward invariant set, an implementation strategy that can guarantee that the closed-loop state is driven into the region where the Safeness Index is less than a desired threshold was presented. Through a chemical process example, the proposed method was demonstrated to be capable of maintaining the closed-loop state within a safe region of operation while maximizing process economics.

Chapter 6 developed sequential and iterative DEMPC's with Safeness Index-based constraints, and implementation strategies for each. Sufficient conditions that guarantee closed-loop stability of a nonlinear process operated under these implementation strategies were derived. A catalytic reactor example was used to compare the two distributed controllers with a cenralized design in terms of computation time, closed-loop performance, and safety constraints satisfaction. The proposed iterative and sequential Safeness Index-based DLEMPC strategies were able to yield comparable closed-loop performance while significantly decreasing the on-line computation time compared to that required to solve the centralized Safeness Index-based LEMPC.

Bibliography

[1] T. M. Ahooyi, M. Soroush, J. E. Arbogast, W. D. Seider, and U. G. Oktem. Model-predictive safety system for proactive detection of operation hazards. *AIChE Journal*, 62:2024–2042, 2016.

[2] AIChE. *Dow's Chemical Exposure Index Guide*. AIChE, New York, New York, first edition, 1994.

[3] AIChE. *Dow's Fire and Explosion Index Hazard Classification Guide*. AIChE, New York, New York, seventh edition, 1994.

[4] A. Alanqar, H. Durand, F. Albalawi, and P. D. Christofides. Integrating production scheduling and process operation via economic model predictive control. In *Proceedings of 55th IEEE Conference on Decision and Control*, pages 3190–3195, Las Vegas, Nevada, 2016.

[5] A. Alanqar, H. Durand, F. Albalawi, and P. D. Christofides. An economic model predictive control approach to integrated production management and process operation. *AIChE Journal*, 63:1892–1906, 2017.

[6] F. Albalawi, A. Alanqar, H. Durand, and P. D. Christofides. A feedback control framework for safe and economically-optimal operation of nonlinear processes. *AIChE Journal*, 62:2391–2409, 2016.

[7] F. Albalawi, A. Alanqar, H. Durand, and P. D. Christofides. Simultaneous control of safety constraint sets and process economics using economic model predictive control. In *American Control Conference*, pages 5062–5067, Boston, Massachusetts, 2016.

[8] F. Albalawi, H. Durand, A. Alanqar, and P. D. Christofides. Achieving operational process safety via model predictive control. *Journal of Loss Prevention in the Process Industries*, in press, 2017.

[9] F. Albalawi, H. Durand, and P. D. Christofides. Distributed economic model predictive control for operational safety of nonlinear processes. *AIChE Journal*, in press, 2017.

[10] F. Albalawi, H. Durand, and P. D. Christofides. Distributed economic model predictive control with Safeness-Index based constraints for nonlinear systems. *Systems & Control letters*, submitted, 2017.

[11] F. Albalawi, H. Durand, and P. D. Christofides. Process operational safety using model predictive control based on a process Safeness Index. *Computers & Chemical Engineering*, 104:76–88, 2017.

[12] F. Alfani and J. J. Carberry. An exploratory kinetic study of ethylene oxidation over an unmoderated supported silver catalyst. *La Chimica e L'Industria*, 52:1192–1196, 1970.

[13] J. T. Allen and N. H. El-Farra. A model-based framework for fault estimation and accommodation applied to distributed energy resources. *Renewable Energy*, 100:35–43, 2017.

[14] F. Alrowaie, R. B. Gopaluni, and K. E. Kwok. Alarm design for nonlinear stochastic systems. In *Proceedings of the World Congress on Intelligent Control and Automation*, pages 473–479, Shenyang, China, 2014.

[15] R. Amrit, J. B. Rawlings, and D. Angeli. Economic optimization using model predictive control with a terminal cost. *Annual Reviews in Control*, 35:178–186, 2011.

[16] R. Amrit, J. B. Rawlings, and L. T. Biegler. Optimizing process economics online using model predictive control. *Computers & Chemical Engineering*, 58:334–343, 2013.

[17] T. L. Anderson, M. Ellis, and P. D. Christofides. Distributed economic model predictive control of a catalytic reactor: Evaluation of sequential and iterative architectures. In *Proceedings of the IFAC Symposium on Advanced Control of Chemical Processes*, pages 26–31, Whistler, Canada, 2015.

[18] D. Angeli, R. Amrit, and J. B. Rawlings. On average performance and stability of economic model predictive control. *IEEE Transactions on Automatic Control*, 57:1615–1626, 2012.

[19] B. M. S. Arifin and M. A. A. S. Choudhury. An alternative approach of risk analysis for multivariable alarm system. *Journal of Chemical Engineering, IEB*, 26:75–79, 2011.

[20] T. I. Bø and T. A. Johansen. Dynamic safety constraints by scenario based economic model predictive control. In *Proceedings of the IFAC World Congress*, pages 9412–9418, Cape Town, South Africa, 2014.

[21] R. Brooks, R. Thorpe, and J. Wilson. A new method for defining and managing process alarms and for correcting process operation when an alarm occurs. *Journal of Hazardous Materials*, 115:169–174, 2004.

[22] D. C. Brown and M. O'Donnell. Too much of a good thing? - Alarm management experience in BP Oil. Part 1: Generic problems with DCS alarm systems. In *Proceedings of the IEE Colloquium on Stemming the Alarm Flood*, pages 5/1–5/6, London, England, 1997.

[23] N. Brown. Alarm management/The EEMUA guidelines in practice. *Measurement and Control*, 36:114–119, 2003.

[24] E. F. Camacho and C. Bordons. *Model Predictive Control*. Springer-Verlag, London, England, second edition, 2007.

[25] Y. Chang, F. Khan, and S. Ahmed. A risk-based approach to design warning system for processing facilities. *Process Safety and Environmental Protection*, 89:310–316, 2011.

[26] X. Chen, M. Heidarinejad, J. Liu, and Panagiotis D Christofides. Distributed economic mpc: Application to a nonlinear chemical process network. *Journal of Process Control*, 22:76–88, 2012.

[27] 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.

[28] P. D. Christofides, J. Liu, and D Muñoz de la Peña. *Networked and distributed predictive control: Methods and nonlinear process network applications*. Springer Science & Business Media, London, 2011.

[29] P. D. Christofides, R. Scattolini, D. Muñoz de la Peña, and J. Liu. Distributed model predictive control: A tutorial review and future research directions. *Computers & Chemical Engineering*, 51:21–41, 2013.

[30] R. W. Chylla, R. A. Adomaitis, and A. Çinar. Stability of tubular and autothermal packed bed reactors using phase plane analysis. *Industrial & Engineering Chemistry Research*, 26:1356–1362, 1987.

[31] A. Çinar, A. Palazoglu, and F. Kayihan. *Chemical Process Performance Evaluation*. CRC Press, Boca Raton, Florida, 2007.

[32] D. A. Crowl and J. F. Louvar. *Chemical Process Safety: Fundamentals with Applications*. Pearson Education, Upper Saddle River, NJ, third edition, 2011.

[33] M. Diehl, R. Amrit, and J. B. Rawlings. A Lyapunov function for economic optimizing model predictive control. *IEEE Transactions on Automatic Control*, 56:703–707, 2011.

[34] EEMUA. *EEMUA-191: Alarm Systems - A Guide to Design, Management and Procurement*. Engineering Equipment and Materials Users Association, London, England, 2013.

[35] N. H. El-Farra and P. D. Christofides. Bounded robust control of constrained multivariable nonlinear processes. *Chemical Engineering Science*, 58:3025–3047, 2003.

[36] M. Ellis and P. D. Christofides. Economic model predictive control with time-varying objective function for nonlinear process systems. *AIChE Journal*, 60:507–519, 2014.

[37] M. Ellis, H. Durand, and P. D. Christofides. A tutorial review of economic model predictive control methods. *Journal of Process Control*, 24:1156–1178, 2014.

[38] S. Gajjar and A. Palazoglu. A data-driven multidimensional visualization technique for process fault detection and diagnosis. *Chemometrics and Intelligent Laboratory Systems*, 154:122–136, 2016.

[39] G. Goble and T. Stauffer. Don't be alarmed: Avoid unplanned downtime from alarm overload, use top techniques to improve alarm management. *InTech Magazine*, 54:42–46, 2007.

[40] J. Gong and F. You. Optimal design and synthesis of algal biorefinery processes for biological carbon sequestration and utilization with zero direct greenhouse gas emissions: MINLP model and global optimization algorithm. *Industrial & Engineering Chemistry Research*, 53:1563–1579, 2014.

[41] L. Grüne. Economic receding horizon control without terminal constraints. *Automatica*, 49:725–734, 2013.

[42] C. He and F. You. Shale gas processing integrated with ethylene production: Novel process designs, exergy analysis, and techno-economic analysis. *Industrial & Engineering Chemistry Research*, 53:11442–11459, 2014.

[43] M. Heidarinejad, J. Liu, and P. D. Christofides. Economic model predictive control of nonlinear process systems using Lyapunov techniques. *AIChE Journal*, 58:855–870, 2012.

[44] R. Huang, L. T. Biegler, and E. Harinath. Robust stability of economically oriented infinite horizon NMPC that include cyclic processes. *Journal of Process Control*, 22:51–59, 2012.

[45] R. Huang, E. Harinath, and L. T. Biegler. Lyapunov stability of economically oriented NMPC for cyclic processes. *Journal of Process Control*, 21:501–509, 2011.

[46] E. A. N. Idris and S. Engell. Economics-based NMPC strategies for the operation and control of a continuous catalytic distillation process. *Journal of Process Control*, 22:1832–1843, 2012.

[47] S. S. Jogwar, M. Baldea, and P. Daoutidis. Dynamics and control of process networks with large energy recycle. *Industrial & Engineering Chemistry Research*, 48:6087–6097, 2009.

[48] M. Kettunen, P. Zhang, and S.-L. Jämsä-Jounela. An embedded fault detection, isolation and accommodation system in a model predictive controller for an industrial benchmark process. *Computers & Chemical Engineering*, 32:2966–2985, 2008.

[49] H. K. Khalil. *Nonlinear Systems*. Prentice Hall, Upper Saddle River, NJ, third edition, 2002.

[50] F. I. Khan and S. A. Abbasi. Major accidents in process industries and an analysis of causes and consequences. *Journal of Loss Prevention in the Process Industries*, 12:361–378, 1999.

[51] K. Kidam and M. Hurme. Analysis of equipment failures as contributors to chemical process accidents. *Process Safety and Environmental Protection*, 91:61–78, 2013.

[52] T. Kletz. *What Went Wrong? - Case Histories of Process Plant Disasters and How They Could Have Been Avoided*. Elsevier, Burlington, Massachusetts, fifth edition, 2009.

[53] P. Kokotović and M. Arcak. Constructive nonlinear control: A historical perspective. *Automatica*, 37:637–662, 2001.

[54] L. Lao, M. Ellis, and P. D. Christofides. Proactive fault-tolerant model predictive control. *AIChE Journal*, 59:2810–2820, 2013.

[55] D. A. Latham, K. B. McAuley, B. A. Peppley, and T. M. Raybold. Mathematical modeling of an industrial steam-methane reformer for on-line deployment. *Fuel Processing Technology*, 92:1574–1586, 2011.

[56] N. Leveson. A new accident model for engineering safer systems. *Safety Science*, 42:237–270, 2004.

[57] N. G. Leveson. *Safeware: System Safety and Computers*. Addison-Wesley, Reading, Massachusetts, 1995.

[58] N. G. Leveson and G. Stephanopoulos. A system-theoretic, control-inspired view and approach to process safety. *AIChE Journal*, 60:2–14, 2014.

[59] Y. Lin and E. D. Sontag. A universal formula for stabilization with bounded controls. *Systems & Control Letters*, 16:393–397, 1991.

[60] P. Liu, E. N. Pistikopoulos, and Z. Li. A multi-objective optimization approach to polygeneration energy systems design. *AIChE Journal*, 56:1218–1234, 2010.

[61] S. Mannan. *Lees' Loss Prevention in the Process Industries - Hazard Identification, Assessment and Control*. Elsevier, Waltham, Massachusetts, fourth edition, 2012.

[62] T. Marlin. Operability in process design: Achieving safe, profitable, and robust process operations. 2012.

[63] J. L. Massera. Contributions to stability theory. *Annals of Mathematics*, 64:182–206, 1956.

[64] 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.

[65] D. I. Mendoza-Serrano and D. J. Chmielewski. Smart grid coordination in building HVAC systems: EMPC and the impact of forecasting. *Journal of Process Control*, 24:1301–1310, 2014.

[66] P. Mhaskar, N. H. El-Farra, and P. D. Christofides. Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. *Systems & Control Letters*, 55:650–659, 2006.

[67] P. Mhaskar, J. Liu, and P. D. Christofides. *Fault-Tolerant Process Control: Methods and Applications*. Springer-Verlag, London, England, 2013.

[68] M. Morari and J. H. Lee. Model predictive control: Past, present and future. *Computers & Chemical Engineering*, 23:667–682, 1999.

[69] I. H. Moskowitz, W. D. Seider, J. E. Arbogast, U. G. Oktem, A. Pariyani, and M. Soroush. Improved predictions of alarm and safety system performance through process and operator response-time modeling. *AIChE Journal*, 62:3461–3472, 2016.

[70] M. A. Müller, D. Angeli, and F. Allgöwer. Economic model predictive control with self-tuning terminal cost. *European Journal of Control*, 19:408–416, 2013.

[71] M. A. Müller, D. Angeli, and F. Allgöwer. On the performance of economic model predictive control with self-tuning terminal cost. *Journal of Process Control*, 24:1179–1186, 2014.

[72] D. Muñoz de la Peña and P. D. Christofides. Lyapunov-based model predictive control of nonlinear systems subject to data losses. *IEEE Transactions on Automatic Control*, 53:2076–2089, 2008.

[73] E. Naghoosi, I. Izadi, and T. Chen. Estimation of alarm chattering. *Journal of Process Control*, 21:1243–1249, 2011.

[74] A. M. Niziolek, O. Onel, M. M. F. Hasan, and C. A. Floudas. Municipal solid waste to liquid transportation fuels - Part II: Process synthesis and global optimization strategies. *Computers & Chemical Engineering*, 74:184–203, 2015.

[75] M. Noda, F. Higuchi, T. Takai, and H. Nishitani. Event correlation analysis for alarm system rationalization. *Asia-Pacific Journal of Chemical Engineering*, 6:497–502, 2011.

[76] B. P. Omell and D. J. Chmielewski. IGCC power plant dispatch using infinite-horizon economic model predictive control. *Industrial & Engineering Chemistry Research*, 52:3151–3164, 2013.

[77] F. Özgülşen, R. A. Adomaitis, and A. Çinar. A numerical method for determining optimal parameter values in forced periodic operation. *Chemical Engineering Science*, 47:605–613, 1992.

[78] A. Pariyani, W. D. Seider, U. G. Oktem, and M. Soroush. Incidents investigation and dynamic analysis of large alarm databases in chemical plants: A fluidized-catalytic-cracking unit case study. *Industrial & Engineering Chemistry Research*, 49:8062–8079, 2010.

[79] J. Prakash, S. C. Patwardhan, and S. Narasimhan. A supervisory approach to fault-tolerant control of linear multivariable systems. *Industrial & Engineering Chemistry Research*, 41:2270–2281, 2002.

[80] S. J. Qin and T. A. Badgwell. A survey of industrial model predictive control technology. *Control Engineering Practice*, 11:733–764, 2003.

[81] J. B. Rawlings and R. Amrit. Optimizing process economic performance using model predictive control. In L. Magni, D. M. Raimondo, and F. Allgöwer, editors, *Nonlinear Model Predictive Control: Towards New Challenging Applications*, pages 119–138. Springer-Verlag, Berlin, Germany, 2009.

[82] J. B. Rawlings, D. Angeli, and C. N. Bates. Fundamentals of economic model predictive control. In *Proceedings of the 51st IEEE Conference on Decision and Control*, pages 3851–3861, Maui, Hawaii, 2012.

[83] D. H. Rothenberg. *Alarm Management for Process Control: A Best-Practice Guide for Design, Implementation, and Use of Industrial Alarm Systems*. Momentum Press, New York, New York, 2009.

[84] R. Scattolini. Architectures for distributed and hierarchical model predictive control- A review. *Journal of Process Control*, 19:723–731, 2009.

[85] H. Smith, C. Howard, and T. Foord. Alarms management/Priority, floods, tears or gain? Introduction to the "problem". *Measurement and Control*, 36:109–113, 2003.

[86] E. D. Sontag. A 'universal' construction of Artstein's theorem on nonlinear stabilization. *Systems & Control letters*, 13:117–123, 1989.

[87] R. R. Tatiya. *Elements of Industrial Hazards: Health, Safety, Environment and Loss Prevention*. CRC Press/Balkema, Leiden, Netherlands, 2011.

[88] A. N. Venkat, I. A. Hiskens, J. B. Rawlings, and S. J. Wright. Distributed MPC strategies with application to power system automatic generation control. *IEEE Transactions on Control Systems Technology*, 16:1192–1206, 2008.

[89] V. Venkatasubramanian, R. Rengaswamy, and S. N. Kavuri. A review of process fault detection and diagnosis: Part II: Qualitative models and search strategies. *Computers & Chemical Engineering*, 27:313–326, 2003.

[90] A. Wächter and L. T. Biegler. On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. *Mathematical Programming*, 106:25–57, 2006.

[91] J. Wang, F. Yang, T. Chen, and S. L. Shah. An overview of industrial alarm systems: Main causes for alarm overloading, research status, and open problems. *IEEE Transactions on Automation Science and Engineering*, 13:1045–1061, 2016.

[92] D. Xue and N. H. El-Farra. Actuator fault-tolerant control of networked distributed processes with event-triggered sensor-controller communication. In *Proceedings of the American Control Conference*, pages 1661–1666, Boston, Massachusetts, 2016.

[93] F. Yang, S. L. Shah, D. Xiao, and T. Chen. Improved correlation analysis and visualization of industrial alarm data. *ISA Transactions*, 51:499–506, 2012.

[94] F. Yang, D. Xiao, and S. L. Shah. Qualitative fault detection and hazard analysis based on signed directed graphs for large-scale complex systems. In W. Zhang, editor, *Fault Detection*, pages 15–50. InTech, 2010.

[95] V. M. Zavala. A multiobjective optimization perspective on the stability of economic MPC. In *Proceedings of the 9th IFAC Symposium on Advanced Control of Chemical Processes*, pages 975–981, Whistler, Canada, 2015.